GLI GLOBAL LEGAL INSIGHTS

Blockchain & Cryptocurrency Regulation

2024

Sixth Edition

Contributing Editor: **Josias N. Dewey**

glg Global Legal Group

ENTERPRISE ETHEREUM ALLIANCE

Value Technology Foundation

WSBA WALL STREET BLOCKCHAIN ALLIANCE

Global Legal Insights
Blockchain & Cryptocurrency Regulation

2024, Sixth Edition
Contributing Editor: Josias N. Dewey
Published by Global Legal Group

GLOBAL LEGAL INSIGHTS – BLOCKCHAIN & CRYPTOCURRENCY REGULATION

2024, SIXTH EDITION

Contributing Editor
Josias N. Dewey, Holland & Knight LLP

Publisher
James Strode

Production Editor
Megan Hylton

Head of Production
Suzie Levy

Chief Media Officer
Fraser Allan

CEO
Jason Byles

We are extremely grateful for all contributions to this edition.
Special thanks are reserved for Josias N. Dewey of Holland & Knight LLP for all of his assistance.

Published by Global Legal Group Ltd.
59 Tanner Street, London SE1 3PL, United Kingdom
Tel: +44 207 367 0720 / URL: www.glgroup.co.uk

ISBN 978-1-83918-306-5
ISSN 2631-2999

Printed and bound by TJ Books Limited
Trecerus Industrial Estate, Padstow, Cornwall, PL28 8RW
October 2023

CONTENTS

Jurisdiction chapters

PREFACE

Regulatory clarity in the digital assets (or crypto) space continues to remain elusive. Nevertheless, interest in regulating digital assets and crypto has never been higher among policymakers and regulators. In the U.S., 2023 saw its most voluminous introduction of bills aimed at regulating the digital asset space. While it is still early days, some U.S. regulators already appear to be approaching digital assets from different and almost combative perspectives (e.g., the Commodities Futures Trading Commission and the Securities Exchange Commission (SEC)). Others, however, appear to be doubling down on their historic approach (e.g., the Department of Justice charging the founders of Tornado Cash with, among other charges, conspiracy to violate money laundering sanctions, a year after placing the virtual currency mixer on OFAC's SDN List). All of this ensures that providing sound legal counsel in this space will continue to be a challenge. Now in its sixth edition, this publication is dedicated to assisting counsel overcome this challenge, whether advising clients in the U.S. or elsewhere.

TThe last year has seen a number of developing trends. First, governments around the world are introducing new laws to adequately regulate the blockchain technology industry. In the United Kingdom, the country's Financial Conduct Authority is launching a crackdown on cryptocurrency companies that violate new stringent marketing and reporting standards. Meanwhile, in the U.S., the SEC is locked in litigious battles with both Coinbase and Ripple, the two biggest cryptocurrency exchanges in the world. Under Chairman Gary Gensler, the regulator's stance appears to be that most crypto tokens are securities and that crypto firms need to first register, or at least talk to regulators, before selling them. Second, Decentralized Finance, or DeFi, has attracted attention from investors and regulators, as the latest and arguably most innovative development in the crypto area. Sitting at the juncture of finance and blockchain technology, DeFi refers to a suite of financial services and products built upon decentralized blockchain networks. What sets DeFi apart is its exclusion of intermediaries, such as banks or traditional financial institutions. In April 2023, the total value locked up in DeFi applications was US$52 billion. Finally, as mainstream consumer confidence in blockchain technology wavers, the value of non-fungible tokens (NFTs) has cratered. In January 2022, Justin Bieber bought a "Bored Ape"

NFT for around US$1.3 million, but it is now worth around US$37,000, down 97%, and still dropping. Furthermore, many NFT companies that published "roadmaps" delineating the company's future plans to increase the value of their NFTs have been targeted by regulators for violating securities and consumer protection laws.

While no publication can provide clarity on all the issues that might be relevant to a digital asset or blockchain engagement, our hope is that this publication frames many of the most significant issues that practitioners will confront. For many issues, clarity is particularly difficult to attain as a result of legislative and regulatory inaction and other gaps in official guidance. As the chapters in this publication reveal, practitioners will generally be well served to approach many of these issues from a technologically agnostic perspective. Laws and regulations serve to advance or implement policies, which are often equally applicable regardless of technology.

There are, however, some instances when a certain aspect of a technology may raise its own unique considerations. For example, "layer 2 blockchain" refers to any off-chain network, system, or technology built on top of a blockchain that helps extend the capabilities of the underlying base layer network (L2 blockchains). New L2 blockchains typically start centralized and aim to gradually become decentralized as adoption increases. Yet, for its creator, the L2 blockchain's native tokens may be considered securities while the blockchain is not sufficiently decentralized. Additionally, many of these L2 blockchains purport to settle transactions between anonymous parties, which will certainly attract governmental scrutiny because of its circumvention of AML/KYC regulations. Hopefully, after digesting the chapters of this publication, the reader will be better able to identify the issues presented by a given engagement and more easily able to properly frame those issues to his or her clients.

Josias N. Dewey
Holland & Knight LLP

GLOSSARY

***Alice* decision**: a 2014 United States Supreme Court decision about patentable subject matter.

Cold storage: refers to the storage of private keys on an un-networked device or on paper in a secure location.

Copyleft licence: the practice of offering people the right to freely distribute copies and modified versions of a work with the stipulation that the same rights be preserved in derivative works down the line.

Cryptocurrencies: a term used interchangeably with virtual currency, and generally intended to include the following virtual currencies (and others similar to these):

- Bitcoin.
- Bitcoin Cash.
- DASH.
- Dogecoin.
- Ether.
- Ethereum Classic.
- Litecoin.
- Monero.
- NEO.
- Ripple's XRP.
- Zcash.

Cryptography: the practice and study of techniques for secure communication in the presence of third parties, generally involving encryption and cyphers.

DAO Report: report issued in July, 2017 by the U.S. Securities and Exchange Commission, considering and ultimately concluding that The DAO (*see below*) was a security.

Decentralised autonomous organisation ("The DAO"): a failed investor-directed venture capital fund with no conventional management structure or board of directors that was launched with a defect in its code that permitted someone to withdraw a substantial amount of the $130,000,000 in Ether it raised.

Decentralised autonomous organisation ("a DAO"): a form of business organisation relying on a smart contract (*see below*) *in lieu* of a conventional management structure or board of directors.

Digital assets: anything that exists in a binary format and comes with the right to use, and more typically consisting of a data structure intended to describe attributes and rights associated with some entitlement.

Digital collectibles: digital assets that are collected by hobbyists and others for entertainment, and which are often not fungible (e.g., CryptoKitties) (*see* **Tokens**, non-fungible).

Digital currency: a type of currency available only in digital form, which can be fiat currency or virtual currency that acts as a substitute for fiat currency.

Digital currency exchange: a business that allows customers to trade cryptocurrencies or digital currencies for other assets, such as conventional fiat money, or one type of cryptocurrency for another type of cryptocurrency.

Digital/electronic wallet: an electronic device or software that allows an individual to securely store private keys and broadcast transactions across a peer-to-peer network, which can be hosted (e.g., Coinbase) or user-managed (e.g., MyEtherWallet).

Distributed ledger technology ("DLT"): often used interchangeably with the term *blockchain*, but while all blockchains are a type of DLT, not all DLTs implement a blockchain style of achieving consensus.

Fintech: new technology and innovation that aims to compete with traditional financial methods in the delivery of financial services.

Initial coin offering: a type of crowdfunding using cryptocurrencies in which a quantity of the crowdfunded cryptocurrency is sold to either investors or consumers, or both, in the form of "tokens".

Initial token offering: *see* **Initial coin offering**.

Internet of Things: a system of interrelated computing devices, mechanical and digital machines, objects, animals or people that are provided with unique identifiers and the ability to transfer data over a network without requiring human-to-human or human-to-computer interaction.

Licences, software: the grant of a right to use otherwise copyrighted code, including, among others:

- Apache.
- GPLv3.
- MIT.

Mining, cryptocurrency: the process by which transactions are verified and added to the public ledger known as the blockchain, which is often the means through which new units of a virtual currency are created (e.g., Bitcoin).

Money transmitter (U.S.): a business entity that provides money transfer services or payment instruments.

Permissioned network: a blockchain in which the network owner(s) decides who can join the network and issue credentials necessary to access the network.

Platform or protocol coins: the native virtual currencies transferable on a blockchain network, which exist as a function of the protocol's code base.

Private key: an alphanumeric cryptographic key that is generated in pairs with a corresponding public key. One can verify possession of a private key that corresponds to its public key counterpart without exposing it. It is not possible, however, to derive the private key from the public key.

Private key storage:

- *Deep cold storage*: a type of cold storage where not only Bitcoins are stored offline, but also the system that holds the Bitcoins is never online or connected to any kind of network.
- *Hardware wallet*: an electronic device capable of running software necessary to store private keys in a secure, encrypted state and structure transactions capable of being broadcast on one or more blockchain networks. Two popular examples are Ledger and Trezor.

Protocols: specific code bases implementing a particular blockchain network, such as:

- Bitcoin.
- R3's Corda.
- Ethereum.
- Hyperledger Fabric.
- Litecoin.

Public network: blockchain that anyone can join by installing client software on a computer with an internet connection. The best known public networks are Bitcoin and Ethereum.

Qualified custodian: a regulated custodian who provides clients with segregated accounts and often places coins or tokens in cold storage (*see above*).

Robo-advice/digital advice: a class of financial adviser that provides financial advice or investment management online, with moderate to minimal human intervention.

Sandbox (regulatory): a programme implemented by a regulatory agency that permits innovative start-ups to engage in certain activities that might otherwise require licensing with one or more governmental agencies.

Security token: a token intended to confer rights typically associated with a security (e.g., stock or bond), and hence, are generally treated as such by regulators.

Smart contract: a piece of code that is written for execution within a blockchain runtime environment. Such programmes are often written to automate certain actions on the network, such as the transfer of virtual currency if certain conditions in the code are met.

Tokens: a data structure capable of being fungible (ERC-20) or non-fungible (ERC-721) that is capable of being controlled by a person to the exclusion of others, which is typically transferable from one person to another on a blockchain network.

Utility token: a token intended to entitle the holder to consume some good or service offered through a decentralised application ("dApp").

Vending machine (Bitcoin): an internet machine that allows a person to exchange Bitcoins and cash. Some Bitcoin ATMs offer bi-directional functionality, enabling both the purchase of Bitcoin as well as the redemption of Bitcoin for cash.

FOREWORD

Dear Innovators,

On behalf of the Enterprise Ethereum Alliance ("EEA"), I would like to thank Global Legal Group ("GLG") for continuing to educate the world on the state of regulation in the blockchain and cryptocurrency sector, with this sixth edition publication of *GLI – Blockchain & Cryptocurrency Regulation*. Once again, GLG has assembled a stable of experts in the legal industry to analyze and explain this complex yet exciting environment.

In 1999, the Dot-Com boom was exciting, inspirational, and full of hype that, if you believed popular media, had run its course by 2001. And yet, over the five years that followed, virtually every business in the modern world added a website to their repertoire. In most cases the sites were simple and static, but that adoption paved the way for the Web2 and app-ecosystem booms that followed. It is during the quiet that the steady progress is made that establishes a new foundation. Having moved through the ICO craze, the L1 explosion, the consumer DeFi boom, the NFT craze, and recently into the L2 scalability boom, blockchain technology has now entered the quiet. Blockchain departments have been slimmed down across the board, but behind the scenes on the technology front we are seeing serious work on both the transaction privacy and individual identity that are needed for widespread enterprise adoption. On the regulatory side, we began to see a patchwork of rulemaking by policy enforcement agencies last year, and this year we are seeing more comprehensive regulatory frameworks such as the European Union's Markets in Crypto-Assets Regulation (MiCA), as well as increasing legislative action efforts in places such as the USA. However, these frameworks and laws so far remain region-specific and untested. We are fortunate to have, in this volume, insights from those on the front lines of this testing. We hope you find them valuable.

Known for developing open blockchain specifications such as the Enterprise Ethereum Client Specification, the Off-Chain Trusted Compute Specification, the EthTrust Specification, and the Cross-chain Interoperability Security Guidelines, the EEA helps its members and the business community through its Ethereum advocacy and trust services, including the aforementioned standards that will increase interoperability and a choice of vendors while lowering costs for its members – the world's largest enterprises and most innovative startups. For additional information about joining the EEA, please reach out to membership@entethalliance.org.

Sincerely,
Daniel C. Burnett, Ph.D.
Executive Director, Enterprise Ethereum Alliance

A look at crypto's horrible, no-good year, and what the future may hold

Ron Quaranta
Wall Street Blockchain Alliance

This 2024 edition of the *GLI – Blockchain & Cryptocurrency Regulation* publication comes at a time of deep uncertainty and continued struggles by participants in the global cryptoasset industry, particularly in the United States. If 2022–2023 represented a "bumpy road ahead", we could easily consider the ensuing months to be what a colleague once described as a "series of potential extinction events". From the collapse of one of the most prominent crypto exchanges (with all of its knock-on effects), to a series of cryptoasset firm bankruptcies, a hostile U.S. administration and a veritable blizzard of regulatory enforcement actions, 2023 has proven to be a make-or-break year for many participants in this industry. And in the wake of all of this, it is important to keep in mind that international markets have continued to evolve and, in many cases, embrace different aspects of cryptoassets and blockchain technology. Venues such as Dubai, Singapore, parts of Europe and the United Kingdom have all put forward regulations, proposed legislation and safe harbors that allow for greater innovation in global markets by leveraging blockchain and cryptoassets. In addition, the possible applications of tokenization, including the tokenization of real-world assets such as real estate, commodities and more, continue to evolve despite an ongoing "crypto winter".

We are privileged at the Wall Street Blockchain Alliance ("WSBA") to have members including banks, brokerage firms, institutional investors, law firms, technology firms and many more, all of which continue to advance the world of crypto and blockchain, and we continue to stand alongside our members and other industry partners as we all chart a path to a crypto and blockchain future. Through this lens, this chapter will highlight some of the more prominent happenings over the past year in the cryptoasset and blockchain arenas. And despite the many pronouncements that "crypto is dead" in the United States, we have found that efforts by legitimate, reasonable participants in the cryptoasset space continue to progress, not least of which in other global markets.

In light of all this, addressing these important developments in turn will hopefully serve as a useful backdrop to the in-depth discussions later in this book.

The fall of FTX

In last year's edition of this book, this chapter touched briefly on the collapse of prominent crypto hedge fund Three Arrows Capital ("3AC"), and how that collapse had a ripple effect that many have said hastened the downfall and bankruptcies of a number of firms, including BlockFi, Celsius, Voyager, and others. While bankruptcy proceedings continue apace for several of these at the time of this writing, the worst was yet to come in the spectacular collapse of the at-the-time second-largest crypto exchange in the world, FTX. Its founder and CEO, Sam Bankman-Fried (also known widely as "SBF"), seemed to be omni-present

in the crypto world, presiding over a growing business that at one point was valued at over $32 billion and growing through an aggressive series of acquisitions and product innovations. With a shock of wild hair and a mild public demeanor, SBF put forward an image of conscientious focus on cryptoassets and the evolution of global markets. He burnished that image with frequent claims to being a proponent of "effective altruism" and pontificating on the importance of collateral and sound business practices to anyone in global financial markets who would listen.[1] Indeed, at the height of his fame and FTX's position in the market, many came to believe that they were seeing a 21st century version of John Pierpont Morgan, as SBF and his firm offered to bail out a number of businesses struggling with the potential of bankruptcy in the still significant wake of 3AC's collapse.[2] But, by the end of 2022 and into early 2023, we would all learn that the truth of all this, as alleged, is much more disturbing than anyone anticipated.

In November of 2022, a prominent crypto news outlet published a report indicating that FTX and an affiliated firm, Alameda Research (a predecessor firm launched by SBF and associates, which operated as a prominent crypto hedge fund), held a significant portion of its overall assets in the FTX "native token", created by the exchange and known as "FTT".[3] In the wake of these reports, the CEO of the world's largest crypto exchange, Binance (himself and his firm now the subject of investigations by regulators at the time of this writing), publicly announced that they would sell their holdings of FTT. This precipitated a "run" on the token, as crypto customers worldwide rushed to unload FTT, and the price collapsed accordingly. The FTX exchange (distinct from FTX.us, a U.S.-based entity) was now unable to meet customer withdrawal demands in the wake of the FTT price collapse. If that wasn't bad enough, Alameda Research, managed by a colleague of SBF's, Caroline Ellison (though ostensibly under SBF's influence or control), borrowed significant amounts of money to fund trading and investments, using the FTT token as collateral for much of this activity.

For a time, additional dramatic developments continued, as Binance's CEO Changpeng Zhao (or "CZ") announced that his firm had signed a letter of intent to acquire FTX. The next day they publicly withdrew their offer, citing, among other things, that FTX had mishandled customer funds.[4] This essentially sealed the fate of FTX, as Bankman-Fried's attempts to raise money from investors to help FTX survive essentially fell on deaf ears. And thus, by November of 2022, FTX had filed for bankruptcy in U.S. courts.

Additional news and research also began to uncover a significant level of overlap between an array of SBF affiliated firms. Some accounts noted that FTX had lent Alameda upwards of $10 billion in FTX customer funds, while other reports indicated that SBF had used up to $100 million of customer funds for political donations.[5] This illicit use of customer assets, along with a wide variety of asset co-mingling allegations across multiple SBF-controlled entities, would become the cornerstone of regulatory and law enforcement actions against FTX and Bankman-Fried.

In early December of 2022, at his home base in the Bahamas, SBF was arrested by Bahamian authorities at the request of the U.S. government and was quickly extradited and charged by U.S. authorities with a multitude of criminal charges, including fraud, conspiracy to commit money laundering, conspiracy to defraud the United States and violations of U.S. campaign finance laws.[6] At the time of this writing, Sam Bankman-Fried sits in a jail cell in New York City awaiting trial, and seems intent on fighting these charges, even as his group of closest advisors has come to plea deals with the government.

There are certainly a great number of steps that brought FTX to this point, many of which will be addressed by fellow authors in this edition. But, suffice to say, the saga is still unfolding,

and will probably make for university case studies for years to come. Its long-term effect on the viability of the crypto markets continues to be the subject of speculation, but no one can deny the deep negative effects that it has had on these markets in the short term.

Revenge of the regulators

A drop in crypto market prices was not the only outcome from the collapse of FTX and other market participants. Indeed, in the wake of these tumultuous events, the position of regulators around the world, many not entirely favorable to crypto, took a significant turn to the downright hostile. Nowhere is this truer than in the United States. And no regulator there has been more hostile than the U.S. Securities and Exchange Commission ("SEC").

In the wake of FTX's collapse, and despite numerous meetings with a wide variety of crypto market participants (including FTX), the SEC, headed by Chairman Gary Gensler, has embarked on the most aggressive series of regulatory enforcement actions against a single industry in most people's memories. From sanctioning alleged unregistered securities exchanges and unregistered securities offerings to alleging fraud and deceptive marketing practices, the agency has launched dozens of cases that have rocked the cryptoasset world, while making him a hero to the fiercest opponents of crypto, particularly in political circles. Indeed, as recently as September of 2023, Chair Gensler was quoted in live testimony giving his oft repeated line that he has "…never seen a field that's so rife with misconduct…".[7] Combined with declarations from the U.S. administration about the risks of crypto, enforcement actions and proposed guidance from a range of other regulatory agencies that make the holding of crypto more difficult, to what many have warned as the "debanking"[8] of legitimate crypto businesses, it is no wonder that America has become decidedly less crypto friendly. Many have taken to calling these events "Operation Chokepoint 2.0", harkening back to the actions during the Obama Administration to investigate banks that conducted business in industries that the current government frowned upon, under the auspices of trying to prevent fraud and money laundering.

But, of course, the world is not only the United States, and it is sensible to give some consideration to the developments that have occurred around the world that may be seen as a bit more accepting of cryptoassets.

For instance, Hong Kong, seemingly looking to become a hub for the global crypto sector, recently issued its first licenses in the summer of 2023 allowing regulated crypto exchanges to offer trading in a number of cryptoassets, including Bitcoin and Ether.[9] The licensing regime is meant to enable strong investor protections, while expanding the city's efforts to bring in fresh capital along with new investment and new talent. Likewise, Japan is working to develop a friendlier but investor protection-focused atmosphere for crypto, even reversing previous rules such as strong capital gains taxes on unrealized cryptoasset profits, which were meant to discourage cryptoasset trading.

Not to be left behind, Europe recently began its countdown to groundbreaking Markets in Crypto-Assets Regulation ("MiCA") licensing regulation, slated for full implementation in 2024.[10] This series of regulations will allow crypto companies like wallet providers, exchanges and more to conduct crypto business across the economic region, while requiring the customer identification, supervision and disclosures that allow for compliant and responsible market participation. While not perfect to many stakeholders, least of all for decentralized finance and privacy purists, rules such as MiCA seem to acknowledge an inevitable future with cryptoassets.

Notably, the United Kingdom also recently passed the Financial Services and Markets Act 2023, which classifies crypto as a regulated financial activity.[11] This law would give the UK Financial Conduct Authority broad oversight of the cryptoasset space, bring stablecoins under its scope as well as crypto marketing promotions and more. While many are not fond of additional regulations, such investor protections are required for an orderly market to develop in a compliant way.

Industry advocates argue that the United States might be well served in taking notice of these developments around the world and considering a regime that enables compliant crypto adoption. This is particularly true in our 21st century where the portability of capital has never been greater, with some warning that the Unites States' hostile stance to innovations like cryptoassets portends a possible future of financial markets that does not necessarily have America as its dominant player.

A long crypto winter

If crypto prices were in bear market territory in late 2022 into 2023, the fall of FTX and the numerous crypto bankruptcies accelerated the drop in those prices, with many tokens still far from their all-time-high prices. While some might consider the crypto winter a "crypto ice age", it is important to remember that innovation keeps moving forward, and builders keep building. From cross-border payments to tokenization to supply chain management using blockchain technology, it is long past the time for detractors to refer to cryptoassets and blockchain as "fringe capabilities" used only for tax evasion and illicit activities.[12] Not all crypto market participants are fraudsters running companies like FTX. For example, multiple global finance organizations are gearing up to launch exchange-traded funds ("ETFs") for spot crypto markets, reflecting institutional and retail client demand for this asset class.[13] (It is worth noting that ETFs based upon futures already exist, though this market segment has little retail engagement, no doubt much to regulators' joy.) In addition, progress continues to be made around the world to launch compliant stablecoins, as well as utilize blockchain technology and tokenization to streamline global cross-border payments,[14] securities issuance[15] and more.

Finally, a critical topic that will be covered by subject-matter experts later in this edition of the book is that of tokenization.[16] Particularly as it relates to real-world assets or "RWA", many believe that tokenization will allow for a wider pool of global citizens to have direct ownership of their assets, thereby disintermediating brokers and other intermediaries. Currently, incumbent business models and their supporters tend to discount the importance of tokenization. However, by lowering costs, improving efficiencies, increasing liquidity, and removing barriers to entry, tokenization offers the promise of wider market access to those who may never have had access to global markets before. When we consider the global plight of the unbanked and underbanked, for example, the usefulness of using blockchain technology for tokenization becomes abundantly clear. Joined with new innovations such as the development of artificial intelligence, Web3 and more, a future of more access, greater financial security, and a wider pool of wealth across the world is indeed a compelling picture for us to paint.[17] It may take some time, but world-changing capabilities often do.

A coming dawn?

In the wake of all of the above, it is important to highlight some important successes that have taken place. For instance, as noted above, we have begun to see the evolution of

proper regulatory regimes and the opportunity for market participants and innovators in financial markets to utilize cryptoassets and blockchain technology to offer services and capabilities that the market needs.

In addition, recent court cases in the United States seem to push back on the growing aggressiveness of regulators such as the SEC, indicating that the Judiciary might be the catalyst to push the government to draft proper cryptoasset and stablecoin regulation.[18]

Ongoing law enforcement work to prevent and punish fraud and other violations is critical. Indeed, all responsible market participants are eager to see appropriate investor protections and safeguards to global market stability. However, a *de facto* ban on crypto activity, particularly activity that is now being embraced by other countries, does not seem to many to be the appropriate way forward.

Long-time industry observers are well aware of the risks as well as opportunities that crypto and blockchain represent. Many of us look forward to a future that works with the best benefits of cryptoassets, tokenization, decentralized finance and more. Such systemic changes require innovative minds, political will, and ultimately patience.

Only then can we put crypto's horrible, no-good year behind us all.

* * *

To continue to aid members and other industry colleagues in understanding the impact of the above events, the WSBA operates with our members across a variety of "Working Groups", each designed to guide, promote, educate, and advocate among and between our member roles, firms, and industries.

With our WSBA Legal Working Group, now totaling more than 200 attorneys and general counsel from more than 100 practices and enterprises globally, we were privileged to continue our work of open commentary and request for information responses with regulators and legislators around the world, including the SEC, the Commodity Futures Trading Commission, and many more. In addition, this group of legal experts discusses the challenges and opportunities available in the cryptoasset world, and how the legal profession can be at the forefront of crypto evolution and adoption.

Our WSBA Accounting Working Group, in cooperation with our accounting members as well as our partners at AICPA and CPA.com, continues to be engaged in and at the forefront of crypto markets, accounting, auditing and taxation. In addition to ongoing Working Group meetings and workshops, the Accounting Working Group has published a series of critical whitepapers to educate the accounting profession worldwide.

The WSBA Enterprise & Technology Working Group continues to serve as the path for partnerships with our members and global technology partners and endures to provide members with a forum to discuss, strategize and collaborate on deep technology solutions and prototypes.

Our Cryptoassets Working Group, which has members from hedge funds to institutional investors to banks and more, continues its work on the institutional adoption of cryptoassets and cryptocurrencies across the world, and has spent significant time and effort analyzing and monitoring the changes in cryptoassets across global marketplaces.

The WSBA Tokenization Working Group continues to focus on the tokenization of both real and virtual assets, the challenges of market adoption, and the unique solutions coming to market almost daily, each of which may enhance and grow the way that assets are created, valued, and traded in a safe and compliant way.

Finally, after extensive work and collaboration with our members and other industry participants, the WSBA was proud to share our proposed "Crypto Industry Principles" Initiative.[19] This important initiative is for consideration by all industry segments, and the principles are designed as foundational statements of best practices, rather than rules for the cryptoasset industry. We continue to work to develop these principles and look forward to furthering collaborations across the globe as the market for cryptoassets and other blockchain-based solutions continues to evolve.

* * *

As we noted in our previous contribution to this publication, law and regulation continue to be core components of the evolution of modern global markets and we continue our work with members and partners around the world to guide and promote the widespread and compliant adoption of cryptoassets and blockchain. The WSBA is once again very proud to stand beside our many members and other global subject-matter experts in contributing to this publication, which continues to be a critical reference for these ever-developing innovations. We look forward to an ongoing dialogue with our colleagues across the spectrum of industries involved including law, banking, trading and more, as we continue to evolve into a crypto and blockchain future.

* * *

Endnotes

1. https://time.com/6262810/sam-bankman-fried-effective-altruism-alameda-ftx
2. https://forkast.news/headlines/sam-bankman-fried-bail-out-blockfi
3. https://www.coindesk.com/business/2022/11/02/divisions-in-sam-bankman-frieds-crypto-empire-blur-on-his-trading-titan-alamedas-balance-sheet
4. https://www.cnbc.com/2022/11/09/binance-backs-out-of-ftx-rescue-leaving-the-crypto-exchange-on-the-brink-of-collapse.html
5. https://www.cnbc.com/2023/08/14/bankman-fried-used-customer-funds-for-100-million-in-us-political-donations-prosecutors-charge.html
6. https://www.theguardian.com/technology/2022/dec/13/sam-bankman-fried-ftx-charged-sec-crypto-exchange
7. https://www.coindesk.com/policy/2023/09/12/gensler-hearing-shows-key-senate-democrat-digging-in-heels-on-crypto
8. https://cointelegraph.com/news/us-house-financial-committee-republicans-look-for-records-to-show-crypto-debanking
9. https://www.bloomberg.com/news/articles/2023-07-05/why-hong-kong-wants-to-be-a-hub-for-the-crypto-sector?embedded-checkout=true
10. https://www.esma.europa.eu/esmas-activities/digital-finance-and-innovation/markets-crypto-assets-regulation-mica
11. https://www.coindesk.com/policy/2023/06/29/uk-crypto-stablecoin-rules-receive-royal-assent-passing-into-law
12. https://insidebitcoins.com/news/senator-sherrod-brown-praises-sec-crackdown-on-crypto-says-ftx-like-problems-are-everywhere-in-crypto
13. https://cointelegraph.com/news/franklin-templeton-files-bitcoin-spot-etf
14. https://www.pymnts.com/digital-first-banking/2023/report-jpmorgan-chase-explores-blockchain-for-cross-border-payments

15. https://www.coindesk.com/consensus-magazine/2023/04/19/blockchain-meets-bonds-how-crypto-can-solve-long-standing-issues-in-capital-markets
16. https://internationalbanker.com/brokerage/asset-tokenisation-blockchains-killer-use-case/#:~:text=Asset%20tokenisation%20allows%20financial%20assets,asset%20on%20the%20token%20holder
17. https://www.nasdaq.com/articles/the-future-of-finance-ai-meets-tokenization
18. https://www.axios.com/2023/08/30/gary-gensler-crypto-court-losses
19. https://www.wsba.co/uploads/3/7/9/4/3794101/final_-_wsba_crypto_industry_principles_-_march_2023.pdf

* * *

Information about the Wall Street Blockchain Alliance can be found at www.wsba.co, or by email to info@wsba.co.

Ron Quaranta
Email: info@wsba.co

Ron possesses over three decades of experience in the global financial services and technology industries. He currently serves as Chairman and Chief Executive Officer of the Wall Street Blockchain Alliance, the world's leading non-profit trade association promoting the comprehensive adoption of blockchain technology and cryptoassets across global markets. Prior to this, Ron served as Chief Executive Officer of DerivaTrust Technologies, a pioneering software and technology firm for financial market participants. Ron is the editor and contributing author of the book "*Blockchain in Financial Markets and Beyond: Challenges and Applications*", published by Risk Books, as well as a contributor to "*GLI – Blockchain & Cryptocurrency Regulation*", published annually by Global Legal Group. He was named in the Top 100 Most Influential People in Accounting by *Accounting Today* in 2018 and is the lead author for the ISACA Blockchain Framework as well as a member of the ISACA Emerging Technology Advisory Group. He is a frequent guest of major media outlets, including Bloomberg Radio, and is a sought-after speaker and writer regarding financial technology and innovation. Ron also serves as an advisor to multiple start-ups and corporations focused on fintech innovation and blockchain technology.

Wall Street Blockchain Alliance

Email: info@wsba.co
URL: www.wsba.co

Blockchain and intellectual property: A case study

Ieuan G. Mahony, Brian J. Colandreo & Jacob Schneider
Holland & Knight LLP

Introduction

As discussed elsewhere in this book, blockchain has the potential for transformational change. Like most transformational technologies, its development and adoption are laden with intellectual property ("IP") issues, concerns and strategies. Further, given the potentially wide-ranging impact of blockchain technology, the public and private nature of its application, and the prevalent use of open-source software, blockchain raises particularly unique IP issues.

The purpose of this chapter is to help the practitioner identify some of the issues that may affect blockchain development and adoption. We address these issues as they may relate to a company's creation of its own IP, and as they may relate to efforts by others to assert their IP against a company. We discuss the issues in the context of the hypothetical scenario discussed below.

The hypothetical transaction

Although many sectors stand to benefit from the use of blockchain technology, the financial and supply chain management sectors may be among the first to benefit. For purposes of discussion, this chapter focuses on the financial sector, and in particular the following hypothetical:

> A U.S. company is building a new platform using distributed ledger technology for its syndicated loan transactions. Many participants are involved in a typical transaction serviced by the platform, including borrowers, lenders, an administrative agent, credit enhancers and holders of subordinated debt. The platform that the company is building employs smart contracts to effectuate the functionality over a permissioned (private) network with several hundred nodes in the network.

Our hypothetical company, as noted, has chosen to deploy its solution via a permissioned network. A blockchain developer has two broad options in this regard. First, the developer could select a public blockchain network for its platform. In a public network, each node contains all transactions, the nodes are anonymous, and participants are unknown to each other. Second, the developer could select a permissioned network (as our hypothetical company has). In a permissioned network, the network owner vets network members, accepts only those that it trusts, and uses an access control layer to prevent others from accessing the network. Unlike the nodes on a public network, the nodes on a permissioned network are not anonymous. In addition, a permissioned network can be structured so that specified transactions and data reside only on identified nodes, and are not stored on all nodes in the network.[1] In certain commercial transactions, participants must be known to each other in order to meet regulatory requirements, such as those designed to prevent money laundering. In these situations, a network of anonymous nodes would not be compliant.

Our hypothetical company has selected a permissioned network, we can assume, to obtain these benefits. This selection comes with costs, however, and the company will lose the benefit, for example, of validating a transaction over the full multitude of distributed nodes in a public blockchain network, and the assurances of immutability that this provides.

The blockchain patent landscape

Since Satoshi Nakamoto published the Bitcoin whitepaper in 2008,[2,3] the number of worldwide blockchain patent applications has grown:

Year	Patent Application Filings (Worldwide)[4]
2013	1
2014	2
2015	72
2016	678
2017	2,374
2018	7,009
2019	10,401
2020	12,551
2021	6,768
2022	3,402

Notably, Chinese entities topped the list of blockchain patent applicants for 2022 (in terms of number of filings), comprising the top four spots overall and eight of the top 10.[5]

The number of issued U.S. patents has likewise grown over time:[6]

Year	Issued Patents
2016	5
2017	19
2018	104
2019	401
2020	1,160
2021	1,823
2022	2,216

The largest holders of these U.S. blockchain patents as of August 2023 are shown below:[7]

Entity	Issued Patents
Advanced New Technologies Co. Ltd.	770
Alibaba Group Holding Ltd.	718
International Business Machines Corp.	700
Bank Of America Corp.	139
Alipay (Hangzhou) Information Technology Co., Ltd.	124
Mastercard International Inc.	117
Accenture Global Solutions Ltd.	95
nChain Licensing AG	95
Capital One Services LLC	88

Because blockchain technology assists in the efficient and secure transfer of assets, it is no surprise that the financial industry is a dominate force in the blockchain patent space. Technology companies like IBM[8] also are utilizing blockchains to improve existing

technologies and processes, including supply chain and digital rights management. The IP holding companies, meanwhile, presumably seek patents solely to monetize them.

What can be protected?

Only new and novel ideas may be patented

Ideas that already are in the public domain may not be patented, and much of blockchain technology falls into that category. As discussed elsewhere in this book, a blockchain is a distributed ledgering system that allows for the memorializing of transactions in a manner that is not easily counterfeited, is self-authenticating, and is inherently secure. The basic concept of a blockchain may not be patented. A ledgering system that records such transactions, employs multiple identical copies of the ledgers, and maintains them in separate and distinct entities, similarly may not be patented as a new and novel idea. Blockchain technology also uses cryptography. Known cryptography techniques, even if used for the first time with blockchain, also are not likely to be patentable unless the combination resulted from unique insights or efforts to overcome unique technical problems.

Anyone is generally free to use these concepts and, as such, they are not patentable. So, what is left that can be protected? Only novel and non-obvious ways to use the above-described blockchain distributed ledger system may be protected. For example, the traditional banking industry utilizes central banks and clearing houses to effectuate the transfer of money between entities, which often results in significant delay to complete the transactions. With access to overnight shipping, real-time, chat-based customer service, and social networks allowing for the live video conferencing of multiple parties positioned around the globe, it is understandable that today's consumer could be disillusioned with the pace at which financial transactions move through the traditional banking industry.

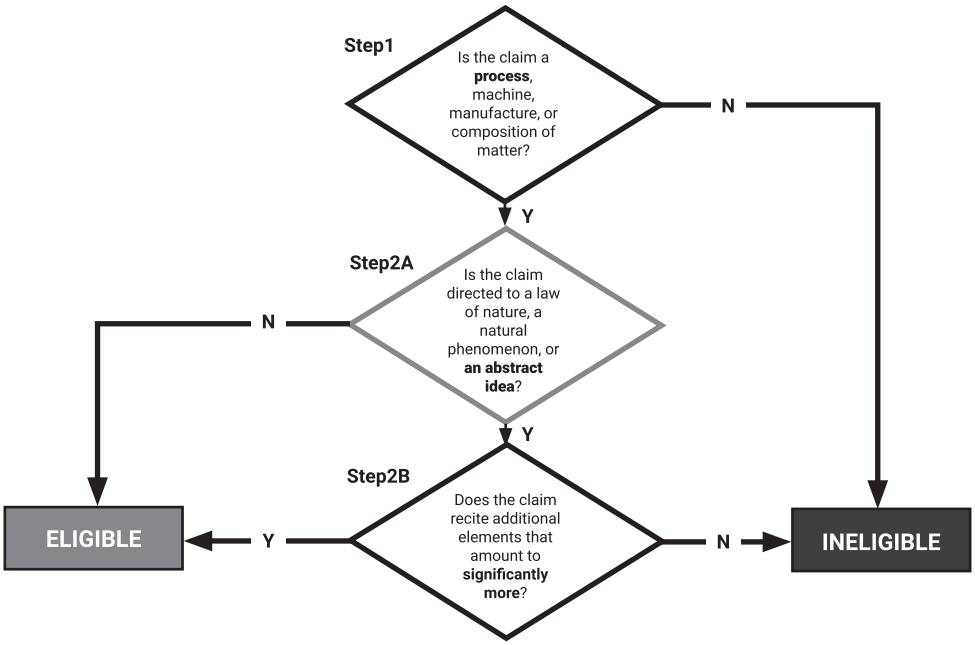
Accordingly, various companies and entities are devoting considerable time and resources to refining and revising the manner in which the traditional banking industry effectuates such monetary transactions. Entrepreneurial companies are inventing unique systems for effectuating asset transfers between banking entities that are memorialized via the above-described blockchain distributed ledgering system, as well as unique systems for expanding the utility of distributed ledgers via remote (and cryptographically secured) content defined within the distributed ledgers. These improvements, as a general proposition, build and improve upon the foundational blockchain technology. Such an improvement could take the form, for example, of an application deployed on the "foundation" of the Hyperledger platform and designed to verify the identity of participants in the hypothetical company's permissioned network, or to create audit trails for transactions on this network. It is these incremental improvements that potentially may be patentable. And it is in this area that our hypothetical company should be focusing its patenting efforts.

The *Alice* decision

Obtaining a patent by our hypothetical company also faces another obstacle. As explained by the Supreme Court in *Alice Corp. v. CLS Bank Int'l*, to be patentable, a claimed invention must be something more than just an abstract idea.[9] Rather, it must involve a technical solution to a specific problem or limitation in the field. In the *Alice* case, for example, a computer system was used as a third-party intermediary between parties to an exchange, wherein the intermediary created "shadow" credit and debit records (*i.e.*, account ledgers) that mirrored the balances in the parties' real-world accounts at "exchange institutions" (*e.g.*, banks). The intermediary updated the shadow records in real time as transactions were entered, thus allowing only those transactions for which the parties' updated shadow records indicated sufficient resources to satisfy their mutual obligations.

The Supreme Court held that, "on their face, the claims before us are drawn to the concept of intermediated settlement, *i.e.*, the use of a third party to mitigate settlement risk." The Court went on to explain that "the concept of intermediated settlement is a fundamental economic practice long prevalent in our system of commerce." The Court then explained that such basic economic principles could not be patented, even if implemented in software or in some other concrete manner, because abstract ideas are not themselves patentable. Allowing patents on abstract ideas themselves, the Supreme Court explained, would significantly restrict and dampen innovation.

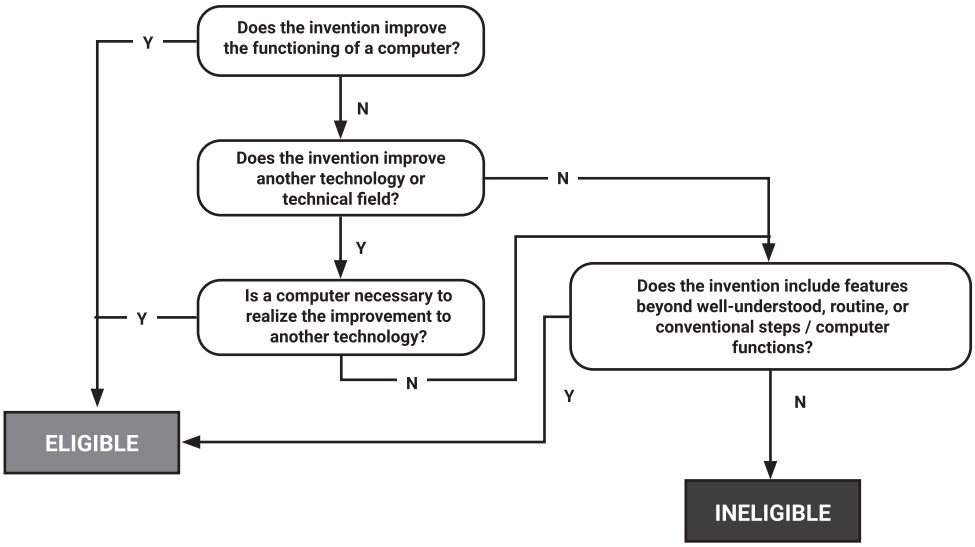
The following flowchart defines the manner in which the patentability of subject matter should be analyzed with respect to the *Alice* decision:



As such, basic concepts, even as they relate to blockchain, may not be patentable. So, our hypothetical company must present more than just basic, economic principles in order to get a patent. It must, for example, claim specific improvements to the functioning of a computer, improvements to other, related technology, effect a transformation of a particular article to a different state or thing, add a specific implementation that is not well understood, routine or conventional, or add unconventional steps that confine the claim to a particular useful application.

Continued overleaf

The following flowchart may be utilized when assessing the patentability of subject matter with respect to the *Alice* decision:



If the *Alice* decision taught practitioners anything, it is that IP law is continuously changing. Accordingly, just as a sound investment plan requires a diversified securities portfolio, a sound IP strategy requires a diversified IP portfolio. Therefore, companies should not put all of their proverbial eggs into one IP basket. For example, if a company was in the "intermediated settlement" space and all they owned were U.S. utility patents, the *Alice* decision would have been devastating to it.

Accordingly, companies should include utility patents in their IP portfolio. But, the prudent company would also include design patents (for protecting, *e.g.*, user interfaces), trade secrets (for protecting, *e.g.*, backend algorithms that are not susceptible to reverse engineering), trademarks (for protecting the goodwill associated with the products produced by the company), service marks (for protecting the goodwill associated with the services provided by the company), copyrights (for protecting software code, and/or the expression of a concept or an idea), and various IP agreements (*e.g.*, employment agreements, development agreements, and licensing agreements). The best IP portfolio for our hypothetical company, therefore, should resemble a quilt that is constructed of various discrete components (utility patents, design patents, trade secrets, trademarks, service marks, copyright, and IP agreements) that are combined to provide the desired level of IP coverage.

The assertion and defense of patent litigation

The threat of patent litigation

Just a few years ago, patent litigation was ubiquitous. Identifying a unique market opportunity, non-practicing entities ("NPEs"), also known as "patent trolls," sprung up, aggregated patents, targeted specific industries, and monetized those patents either through threats of litigation or actual lawsuits. One sector that was the subject of this attack was the telecommunications industry. Beyond a number of competitor *versus* competitor suits (such as *Apple v. Samsung*), large, sophisticated NPEs also arose that did not make a product or sell a service. Rather, they purchased patents, created portfolios, and engaged in litigation

campaigns to force companies to pay royalties on those patents. Often, if an NPE had a large enough portfolio, then a company would enter into a license agreement to license that portfolio for a defined period of time, often five years.

In the last few years, patent litigation has waned. Due to Congress's creation of *inter partes review* ("IPR") proceedings, stricter requirements on proving damages, member organizations that acquire patents and offer licenses to their members, restrictions on where patent lawsuits may be filed, and new defenses that more easily allow patents to be invalidated at the early stages of litigation, patent litigation is no longer the economic opportunity that it previously had been. While competitors still will engage in patent litigation to preserve (or attack) their relative positions in the marketplace, NPEs have found that this changing landscape has made patent litigation financially less rewarding. To be sure, such patent litigation still exists. Indeed, new lawsuits are filed daily. The number and threat of those lawsuits has greatly diminished, however, and the value of patents generally has diminished as well.

Market changes, of course, can create new incentives for initiating patent litigations, and the increased role of blockchain technology is likely to bring about one of those changes. To the extent blockchain technology becomes prevalent, it is likely to result in substantially increased patent litigation, both between competitors and between NPEs and practicing companies. The reasons for this potential change are several:

- In a competitive landscape, certain companies – specifically those technology companies solely directed toward creating blockchain products – must use their patents to keep competitors out of the marketplace.
- Blockchain is ushering in a new set of patents, based on new technology, that have not been licensed.
- Blockchain technology will be used in lucrative fields, which, by association, will make blockchain patents more valuable.
- Blockchain technology likely will be used as fundamental building blocks, making the technology more valuable and damages more lucrative.
- Blockchain startups that hold patents may fail, which could put those patents in the hands of an NPE.

Certainly, NPEs see the opportunity. Eric Spangenberg, a well-known founder of NPEs, has set up IPwe to collect and exploit blockchain patents, and Intellectual Ventures, a well-known and well-financed NPE, similarly is seeking to acquire and exploit patents in this area.[10] And our hypothetical transaction platform reflects this opportunity. If our hypothetical company builds blockchain technology into the basic building blocks of its transactions, and its transactions form the basic building blocks of its business, then it stands to reason that the technology underlying those activities has significant value.

Offensive and defensive uses of patent rights

When entering into this new technical field, therefore, it is critical that our hypothetical company understands the patent landscape. Are there so many patents that they create a barrier to entry? Are other companies actively applying for patents? If so, are they doing so to block others or require licensing fees, or are they doing so merely for defensive purposes? Understanding and properly predicting this landscape may be the difference between a successful and a failed endeavor.

Broadly speaking, the strategic use of patent rights can be categorized as offensive or defensive (or a mix of the two). These strategies are discussed in greater detail below.

Offensive uses of patent rights

From an offensive perspective, the holder of a patent gains the right to exclude others from making, using or selling the invention.[11] An offensive patent holder therefore has the ability

to block all others from utilizing its patented inventions. In an emerging technical field like blockchain, patent filers typically have a more open landscape of new solutions to discover and claim. Because of the patent holder's right to exclude, each solution it is able to patent can block competitors from utilizing that solution in their own products or services absent permission.

For our hypothetical company, if the patented technology allows for a more efficient and secure transaction, then our hypothetical company may want to exclude others from using that technology, giving the hypothetical company a competitive advantage in the marketplace. If our hypothetical company does not wish to exclude competitors, it may instead allow other companies to use its patented technology, but demand that they pay reasonable royalties for that use, perhaps to help defray research and development costs or to create an alternative revenue stream.

It is not enough, however, for the offensive patent holder to file and receive issued patents. The offensive patent holder must affirmatively enforce its patent rights, and make sure that those patent rights are not encumbered by open-source licenses, as per our discussion in "The impact of open-source software" section, or by FRAND licensing obligations, as per our discussion in "The role of industry standards" section. Enforcement requires monitoring for activities that may infringe the patent holder's claims, demanding that others halt infringing activities and, if necessary, instituting litigation to halt the activities by and/or receive reasonable compensation for those activities.

Our hypothetical company also may seek to develop income streams from its patent portfolio. By enforcing its patent rights, the offensive patent holder may force competitors to take and pay for licenses. These licenses may provide income to the offensive patent holder as a single lump sum, where the licensee pays for its license upfront, or as a running royalty, where the licensee pays a percentage of the revenue generated by its products in the marketplace.

Defensive uses of patent rights

Rather than affirmatively asserting patents, the defensive patent holder uses them as a hedge against other potential claims against it. Thus, if the hypothetical company is building a platform and cannot have that platform's use interrupted, then the hypothetical company needs to build up as many defenses against a claim of patent infringement as possible. By having its own portfolio, our hypothetical company may be able to deter competitors from a lawsuit against it, because that competitor knows that it may face claims against it if it brings a patent infringement action.

A defensive strategy, if timely performed, also can block others from securing patents that later can be asserted against it. That is, in fact, the precise strategy of Coinbase's patent filings. By filing for as many patents as possible in the blockchain field, Coinbase hopes to take away patent rights from NPEs, which those entities could otherwise assert against Coinbase.[12]

Ultimately, as blockchain matures, players in the field will tend to take several forms. Patent leaders will emerge, and to avoid mutual destruction, they will enter into cross-licenses with each other. Other companies will try to enter the industry without a proper patent portfolio, and may find significant barriers to entry if the existing patent leaders seek to assert their right to exclude those other companies from using their patented technology. And then there will be companies that simply acquire patents for the purpose of asserting them. Such companies will create transaction costs but should not bar entry into the marketplace.

* * *

Our hypothetical company must then consider a long-term strategy. Is it creating a platform of critical importance, but leaving itself vulnerable to its competitors? Is it fully taking

advantage of its hard work and innovation by protecting the original and novel concepts that it created? Will it find itself blocked by aggressive competitors that are aggregating important patents? All of these questions must be addressed at the same time that our hypothetical company is investing in its technological improvements, and seeking to attract entities and (perhaps) developers to join and participate in its newly created blockchain network.

Strategies for limiting patent litigation exposure

The threat of patent litigation in the blockchain field is real. So how can our hypothetical company limit potential liability? There are several steps that it can take:

- **Open-source defenses**. At a minimum, if a claim is asserted, our hypothetical company needs to consider whether that claim is blocked or barred by open-source restrictions. In addition, our company also should be deliberating carefully on its own open-source strategy, and how the use of open-source software impacts its potential defenses and assertion rights.
- **Actively enter into cross-license agreements**. If our hypothetical company has acquired a significant patent portfolio, then it may want to approach other major players in the blockchain field and seek to enter into cross-licenses with those companies. This approach allows companies to compete based on the quality of their product or service, rather than engage in a damaging patent war.
- **Join patent pools**. In certain industries, particularly telecommunications, patent pools have arisen to help combat NPEs. These patent pools are membership-based organizations, whereby companies pay a fee for a license to all patents held by the pool. The patent pool's typical approach is to acquire patents, or take licenses on patents, for the benefit of its members. The goal of these organizations is to charge a reasonable fee for a license to a broad-based portfolio.
- **Monitoring patent application and allowed patents**. If committed, our hypothetical company can review patent applications as they are published (18 months after filing) and when patents issue (on average 23.3 months after filing).[13] Doing so allows a company to identify potentially problematic patents. The downside of such an approach, however, is that such monitoring may become discoverable in a patent litigation, and perhaps can be used as evidence of knowing (willful) infringement.
- **Consider design arounds where available**. To the extent our hypothetical company identifies potentially problematic patents or applications, an option for it is to "design around" the problematic patent. In other words, our hypothetical company can analyze the particular elements that make up the invention, and eliminate one or more of those elements in its product in order to avoid practicing the patent.
- **Be prepared to file IPRs**. If our hypothetical company finds a problematic patent, then one option is to file an IPR with the Patent Office to try to invalidate the patent. Our hypothetical company can take that step even if no lawsuit has been filed against it. Deciding whether to do so requires an assessment of the likelihood that the patent can be invalidated and the cost associated with that process, but that cost will always be substantially less than the cost of patent litigation.
- **Be prepared to attack the patents on *Alice* grounds**. If our hypothetical company ends up in litigation, it still may be able to terminate that litigation early by filing an *Alice* motion, discussed more fully in the "Offensive and defensive uses of patent rights" section above. The blockchain concept itself is an abstract idea, and not patentable as such. To have a valid blockchain patent, the claimed idea must identify some technical problem in the field and provide some specific technical solution to that problem. Without providing something sufficiently concrete, our hypothetical company may be able to invalidate the asserted patent early in the litigation process.

- **Assert counterclaims**. As discussed above, it is important for our hypothetical company to acquire its own patent portfolio. If successful in doing that, and if sued by a practicing company, then our hypothetical company may be able to assert its own claims of patent infringement. Doing so typically makes it easier to resolve a dispute in its early stages.

The impact of open-source software

The term "open-source software" refers to software that is distributed in source code form. In source code form, the software can be tested, modified, and improved by entities other than the original developer. The term "proprietary" software refers to software that, in contrast, is distributed in object code form only. The developer of proprietary software protects its source code as a trade secret, and declines to allow others to modify, maintain, or have visibility into its software code base. Proponents of open-source software state that the structure fosters the creation of vibrant – and valuable – developer communities, and leads to a common set of well-tested, transparent, interoperable software modules upon which the developer community can standardize.

Open-source software is ubiquitous in blockchain platforms. The software code bases for Bitcoin,[14] public Ethereum,[15] and Hyperledger,[16] and portions of the software code bases for Enterprise Ethereum[17] and Corda,[18] all consist of open-source software. Bitcoin and Ethereum are the leading public blockchain platforms, and Hyperledger, Corda, and Enterprise Ethereum are the "big three" leading commercial, permissioned blockchain platforms.[19] Accordingly, if our hypothetical company wishes to leverage solutions that rely on software from any of these leading platforms, it must consider the impact of the licenses that govern this software.

The open-source community has developed a number of licenses, and these range from (a) permissive licenses, which allow licensees royalty-free and essentially unfettered rights to use, modify, and distribute applicable software and source code,[20] to (b) restrictive, so-called "copyleft" licenses, which place significant conditions on modification and distribution of the applicable software and source code. Two open-source licenses are particularly relevant to our hypothetical company: the General Public License version 3 ("GPLv3"),[21] because this license (and variants) governs large portions of the Ethereum code base;[22] and the Apache 2.0 license ("Apache License"),[23] because this license governs open-source software provided via the Hyperledger, Corda, and Enterprise Ethereum platforms.[24] Each of these licenses embodies a "reciprocity" concept that our hypothetical company must consider.

GPLv3 is known as a "strong" copyleft license. The license functions as follows: assume a developer is attracted to a software module subject to GPLv3, and incorporates this module into proprietary software that he or she then distributes to others. To the extent the developer's proprietary software is "based on" the GPLv3 code,[25] the developer is required to make his or her proprietary code publicly available in source code form, at no charge, under the terms of GPLv3. This requirement will remove trade secret protection embodied in the proprietary code, as well as the developer's ability under copyright law to control the copying, modification, distribution, and other exploitation of its software.[26] This license, therefore, has a significant impact on the developer's trade secret and copyright portfolios.

GPLv3 also has a significant impact on the developer's patent portfolio. The license obligates the developer to grant to all others a royalty-free license to patents necessary to make, use, or sell the Derivative Code.[27] Finally, simply by distributing GPLv3 code, without modification, the developer agrees to refrain from bringing a patent infringement suit against anyone else using that GPLv3 code.[28] In sum, the structure of GPLv3 reflects a strong "reciprocal"

concept: if a developer wishes to incorporate open-source software into its code base, it must reciprocate by contributing that code base (and all needed IP rights) back to the community. As noted above, the Ethereum code base is licensed predominantly under GPLv3. Therefore, our hypothetical company should use caution in relying on Ethereum code.

Our hypothetical company should also consider the impact on its IP portfolio of relying on Hyperledger, Corda, and Enterprise Ethereum code. The Apache License (or an equivalent) governs large portions of these code bases. For our hypothetical company, although the Apache License has reciprocal features, it is considerably more flexible than GPLv3. The Apache License impacts a developer's rights to its software under patent, trade secret, and copyright law in a manner similar to GPLv3;[29] however, these impacts only arise where the developer affirmatively contributes its software to the maintainer of the Apache code at issue. The structure functions with respect to patents as follows: if a patent owner contributes software to an Apache project, the Apache License restricts the owner from filing a patent infringement claim against any entity based on that entity's use of the contributed software. If the owner does bring such a suit, the owner's license to the Apache code underlying its contribution terminates.[30] The license thus has a reciprocal structure: a patent owner cannot benefit from Apache-licensed software while suing to enforce patents that read on its contributions to the Apache software community. If the developer, however, decides not to contribute its code to an Apache project, the developer remains free to incorporate Apache code into its proprietary code base, and commercialize this code without obligation to the Apache open-source community. The Apache License, therefore, provides developers with considerable flexibility.[31]

This flexibility may present strong value to our hypothetical company. It would permit the company, for example, to leverage existing Apache-licensed software from the Hyperledger, Corda, and Enterprise Ethereum code bases in order to develop its new platform and applications, and would give the company full control over whether and to what extent it wishes to encumber its IP portfolio with open-source obligations.

Based on the above, it might appear that our hypothetical company would take extreme steps to avoid GPLv3 code (or other strong copyleft code) and would never contribute code to an Apache project. This, however, has not been the case. A number of entities have contributed code under the Apache License, for example, in order to encourage developers and users to adopt the permissioned commercial network that implements this code.[32] Our hypothetical company will similarly want to consider the potential benefits of seeking to create a vibrant developer and user community using an "open" approach to its IP portfolio, and potentially contributing code under an appropriate open-source software license. In any event, open-source software licenses and licensing techniques play a key role in blockchain technology, and our hypothetical company will want to carefully consider these licenses and techniques in its IP strategy.

The role of industry standards

Background

Industry standards refer to a set of technical specifications that a large number of industry players agree upon to use in their products.[33] Industry players collaboratively develop these technical specifications in a Standards Setting Organization (or "SSO"). Periodically, the SSO will hold meetings where participants, often scientists and engineers, who represent industry players will propose and debate differing proposals for how a technology should operate. Decisions regarding proposals, and the final technical specifications that stem from them, are reached by consensus of the participants.

Current efforts to standardize blockchain technology

Several organizations have begun standardizing a variety of blockchain technologies:

- The International Standards Organization ("ISO") has formed Technical Committee 307 ("ISO/TC 307") to consider blockchain and distributed ledger technologies.[34]
- The Institute of Electrical and Electronics Engineers ("IEEE") has formed two blockchain groups: (1) Project 2418 to develop a standard framework for the use of blockchain in Internet-of-Things applications;[35] and (2) Project 825 to develop a guide for interoperability of blockchains for energy transaction applications.[36]
- The Blockchain in Transportation Alliance ("BiTA") is focused on the use of blockchain in freight payments, asset history, chain of custody, smart contracts and other related goals.[37]
- Hyperledger is a blockchain standard project and associated code base hosted by the Linux Foundation that focuses on finance, banking, Internet-of-Things and manufacturing.[38]
- The Enterprise Ethereum Alliance recently released an architecture stack designed to provide the basis for an open-source, standards-based specification to advance the adoption of Ethereum solutions for commercial, permissioned networks (referred to as "Enterprise Ethereum").[39]

Advantages and disadvantages of standards

Advantages of using and contributing to industry standards

There are several advantages to using standards that benefit an industry at large:

- **Ensures product compatibility** – With a standard in place, any vendor can develop a product that will be compatible with other products in the industry.
- **Stronger technology** – Technical specifications created with the input of many industry players tend to result in stronger overall technologies. In theory, the best ideas should emerge from the process and become industry standards that benefit both vendors and consumers.
- **Shifts competition from the standardized technology to implementation** – Standardization allows industry players to avoid competition with regard to the standardized technology, and instead shift their focus to developing the best implementation of the remaining technology. Entities that participate in the standard-setting process are obligated to disclose patents that are essential for implementing the standard, and to provide licenses to these patents on fair, reasonable, and non-discriminatory terms (so-called "FRAND" terms). These FRAND obligations ensure that all implementers will bear the same licensing burden as to patents essential to the standard.
- **Greater likelihood of wide adoption** – Approval by many industry players makes the standardized approach a "safer bet" for technology adopters and investors.

Contributing to SSOs also yields several benefits to individual participants. First, a participating company gains visibility into what comes next in their industry. For example, a software vendor for a syndicated loan blockchain platform could observe the emerging form and content of the blockchain's smart contracts and begin to steer its internal development toward efficiently processing those contracts. Second, a participating company has the opportunity to guide the standardization process. For example, steering the SSO toward smart contracts that reference cloud-based digital documents would be advantageous for a vendor with a strong cloud-based solution in place.

Disadvantages of using and contributing to industry standards

There are disadvantages to employing industry standards as well. First, a company loses control over certain aspects of the technology. Instead of developing technology

in isolation, our hypothetical company can be at the whim of the industry and its own competitors. Second, a company could develop its own technology that wins over others' in the marketplace. Good faith participation in an SSO implies that a company will contribute its best, most valuable ideas to the SSO instead of applying them solely to its own products. But the prize for developing better technology than the SSO's participants, and not contributing it to the SSO, is alluring: a lucrative monopoly on the best technology. Third, an SSO is less nimble than an individual company because changes to industry standards take consensus of many parties, which in turn take time. Finally, by participating in the SSO process, the company will place FRAND obligations on any patents in its portfolio that are essential for purposes of implementing the standard.

Lessons from wireless telecommunications industry standards

Blockchain technology is a relatively new field, and SSOs are only starting to form to develop blockchain standards. Many companies are now deciding whether to join a blockchain SSO or pursue their own solutions. The history of another technical field's telecommunications and standardization activities provides a good example of the advantages and disadvantages of pursuing industry standards or deciding to go it alone.

In order for a phone to access a carrier's wireless network, it must know how to communicate with the carrier's network. Telecommunications standards dictate how that communication proceeds. By adhering to the telecommunications standard, a manufacturer can ensure that its phone can operate on any carrier's wireless network that also follows that standard.

In the 1980s, the European "first-generation" wireless telecommunications market was fractured by a handful of standards marked by national or regional boundaries. Scandinavia used a standard called "NMT;" Great Britain used "TACS;" Italy used "RTMS" and "TACS;" France used "RC2000" and "NMT;" and Germany used "C-Netz."[40] Using this hodgepodge of telecommunications standards meant that a German's phone would not work during her vacation to France, and an Englishman's phone would not work in Scandinavia.[41] Manufacturers for both phones and network infrastructure were likewise geographically constrained. These manufacturers would typically only research and develop products for specific European regions. What resulted were regional monopolies for those manufacturers, but with low subscriber rates and little opportunity to compete in foreign markets where their technology would be inoperable.[42]

Mindful of these issues with the first-generation wireless telecommunications standards, phone and infrastructure manufacturers from around Europe (and indeed around the world) came together to develop a pan-European, "second-generation" standard within the European Telecommunications Standards Institute ("ETSI") SSO. These manufacturers sent their best scientists and engineers to ETSI to ensure that this emerging standard would meet wireless subscribers' and carriers' needs. The result of their work was the Global System for Mobile Communications ("GSM"), which was the *de facto* wireless standard throughout Europe and parts of the United States from 1992 through 2002. During that period, manufacturers would compete to develop better phones or network equipment, all the while maintaining compliance with the GSM standard. As a result, equipment developed in Sweden or Finland could be sold throughout Europe. This open market brought the price of wireless technology down, increased subscriber bases and, by adoption of a similar approach in the United States, ushered in today's ubiquitous smartphones and wireless networks.

Analogies can be drawn to current trends in blockchain standardization. Blockchain is based on networks that are large enough – have enough nodes – to create reliability. As such, interoperability and scalability are important. Standardization of blockchain elements can be an important tool in achieving those goals, but the standardization process often

involves competing visions. Certain companies will advance one approach, and other companies will advance a different approach. This advocacy typically is based on a good faith belief, but it also arises from investments that companies make in their technology.

A meaningful standardization process contains both risk and opportunity for our hypothetical company. No company wants to make the wrong bet and become the "Betamax" or "HD DVD" of blockchain technology. Companies therefore need to be thinking hard about the competing standards that are being created and what role they wish to play in that creation. An entirely passive role can result in other thought leaders seizing the marketplace, but too aggressive a role can lead to massive investments that are not adopted by the marketplace as a whole. Ultimately, every company needs to think about the role that they wish to play on that spectrum.

* * *

Endnotes

1. There are a range of other differences between public and permissioned networks as well. For example, a permissioned network can be structured with different consensus rules that reduce the resource requirements (including electricity requirements) needed on a public network such as Bitcoin. There are also a range of gradations between fully public and fully private blockchain networks. The Enterprise Ethereum Alliance, for example, is designed to permit operation on a public network, but to restrict the nodes on that public network that receive the data at issue. *See* I. Allison, Enterprise Ethereum Alliance Is Back – And It's Got a Roadmap (May 2, 2018), located at https://www.coindesk.com/enterprise-ethereum-alliance-isnt-dead-got-roadmap-prove
2. Nakamoto, Satoshi, Bitcoin: A Peer-to-Peer Electronic Cash System (October 31, 2008) (located at https://bitcoin.org/bitcoin.pdf).
3. 2008 is not the earliest disclosure of blockchain-like solutions. *See* Stuart Haber and W. Scott Stornetta (1991) and Bayer, Haber and Stornetta (1992).
4. https://www.lens.org (using the search terms "blockchain" or "distributed ledger" in the fields Title, Abstract or Claims). The numbers also only reflect the data available as of August 2023. The drop off in 2022 is likely explained by the lag of 2022 patent application filings being published or issued, particularly when Chinese entities top the list of patent applicants for 2022 and Chinese applications take 18 months to publish upon filing. *See* When is a Chinese patent application published by the Chinese Patent Office?, China Patent Agent (H.K.) Ltd. (https://www.cpahkltd.com).
5. https://harrityllp.com/titans-of-technology-blockchain-the-top-companies-in-blockchain-patents-2021
6. https://www.lens.org/lens/search/patent (using the search terms "blockchain" or "distributed ledger" in the fields Title, Abstract or Claims, with the United States jurisdiction filter).
7. https://www.lens.org/lens/search/patent (using the search terms "blockchain" or "distributed ledger" in the fields Title, Abstract or Claims, with the United States jurisdiction filter).
8. https://www.ibm.com/blockchain
9. *Alice Corp. v. CLS Bank Int'l*, 134 S. Ct. 2347 (2014).
10. Certain industry participants have been working to place restrictions on key patents, to prevent them from being acquired by NPEs. *See* Michael del Castilloite, Patent Trolls Beware: 40 Firms Join Fight Against Blockchain IP Abuse (March 16, 2017), located at https://www.coindesk.com/40-blockchain-firms-unite-in-fight-against-patent-trolls

11. 35 U.S. Code § 154(a)(1) ("Every patent shall . . . grant to the patentee, his heirs or assigns, of the right to exclude others from making, using, offering for sale, or selling the invention throughout the United States or importing the invention into the United States . . .").
12. https://blog.coinbase.com/how-we-think-about-patents-at-coinbase-26d82b68e7db
13. FY 2020, Performance and Accountability Report, U.S. Patent and Trademark Office, https://www.uspto.gov/sites/default/files/documents/USPTOFY20PAR.pdf
14. *See* https://www.Bitcoin.org
15. L. Zeug, "Licensing" (September 4, 2016), located at https://github.com/ethereum/wiki/wiki/Licensing
16. "About Hyperledger," located at https://www.hyperledger.org/about
17. Enterprise Ethereum Alliance Specification Clears the Path to a Global Blockchain Ecosystem (May 16, 2018), located at https://entethalliance.org/enterprise-ethereum-alliance-specification-clears-path-global-blockchain-ecosystem
18. "Contributing to Corda," located at https://github.com/corda/corda/blob/master/CONTRIBUTING.md; Downloads: DemoBench for Corda 3.0, located at https://www.corda.net/downloads
19. R. Brown, "Corda: Open Source Community Update" (May 13, 2018), located at https://medium.com/corda/corda-open-source-community-update-f332386b4038
20. Bitcoin software, for example, is licensed under the permissive MIT License. *See* https://www.Bitcoin.org; https://opensource.org/licenses/MIT
21. GPLv3 license, located at https://www.gnu.org/licenses/gpl-3.0.en.html
22. L. Zeug, "Licensing" (September 4, 2016), located at https://github.com/ethereum/wiki/wiki/Licensing. *See*, *e.g.*, Ethereum-sandbox License, located at https://github.com/ether-camp/ethereum-sandbox/blob/master/LICENSE.txt
23. Apache 2.0 license, located at https://www.apache.org/licenses/LICENSE-2.0
24. For Corda, *see* R. Brown, "Corda: Open Source Community Update" (May 13, 2018), located at https://medium.com/corda/corda-open-source-community-update-f332386b4038; "Contributing to Corda," located at https://github.com/corda/corda/blob/master/CONTRIBUTING.md. For Hyperledger, *see* Brian Behlendorf, "Meet Hyperledger: An 'Umbrella' for Open Source Blockchain & Smart Contract Technologies" (September 13, 2016), located at https://www.hyperledger.org/blog/2016/09/13/meet-hyperledger-an-umbrella-for-open-source-blockchain-smart-contract-technologies. Code contributed to the Enterprise Ethereum Alliance is generally made available under an open-source license that mirrors the Apache 2.0 license, *see* Enterprise Ethereum Alliance Inc. Intellectual Property Rights Policy, located at https://entethalliance.org/join
25. In defining the key term "based on," GPLv3 largely relies on copyright law rules governing derivative works. Courts generally rule that two copyrighted works are distinct (and one is not derivative of the other) if "they can live their own copyright life;" in other words, the test focuses on whether each expression "has an independent economic value and is, in itself, viable." *E.g.*, *Columbia Pictures Indus. v. Krypton Broad. of Birmingham, Inc.*, 259 F.3d 1186, 1192 (9th Cir. 2001); *Lewis Galoob Toys, Inc. v. Nintendo of America, Inc.*, 964 F.2d 965, 969 (9th Cir. 1992).
26. For convenience, the code the developer is required to open-source in this manner is referred to as "Derivative Code."
27. GPLv3, sec. 11 (Patents).
28. GPLv3, sec. 10 (Automatic Licensing of Downstream Recipients).
29. The maintainer of the relevant Apache code at issue, through the Apache Software Foundation, has the ability to set downstream terms for the contributed software.

30. Apache 2.0, sec. 3 (Grant of Patent License).
31. Our hypothetical company will also need to consider "compatibility" issues between various open-source licenses. The Hyperledger platform, for example, was unable to assimilate Ethereum code due to incompatibility between the Apache License and strong copyleft licenses, and the resulting need to obtain permissions from copyright owners to "re-license" the Ethereum code at issue. *See* J. Manning, Hyperledger Fails Ethereum Integration Due To Licensing Conflicts (February 3, 2017), located at https://www.ethnews.com/hyperledger-fails-ethereum-integration-due-to-licensing-conflicts; J. Buntinx, Ethereum app Developers may Face Licensing Issues Later on (December 6, 2017), located at https://www.newsbtc.com/2017/12/06/ethereum-app-developers-may-face-licensing-issues-later
32. IBM, for example, has contributed code under the Apache License to the Hyperledger platform, and in turn is providing commercial Blockchain-as-a-Service ("BaaS") offerings based on this platform using IBM's cloud infrastructure. *See* IBM Blockchain, The Founder's Handbook: Your guide to getting started with Blockchain (Edition 2.0), located at https://www-01.ibm.com/common/ssi/cgi-bin/ssialias?htmlfid=28014128USEN. Microsoft has similar commercial offerings, based on Azure and the Enterprise Ethereum platform. *See* M. Finley, Getting Started with Ethereum using Azure Blockchain (January 24, 2018), located at https://blogs.msdn.microsoft.com/premier_developer/2018/01/24/getting-started-with-ethereum-using-azure-blockchain
33. A simple example is the shape and voltage of a wall power outlet. Because the power outlet is standardized among geographic regions, an appliance maker can ensure that its coffee maker will work (and can be sold) anywhere within a given region.
34. https://www.iso.org/committee/6266604.html
35. https://standards.ieee.org/develop/project/2418.html
36. https://standards.ieee.org/develop/project/825.html
37. https://bita.studio
38. https://www.hyperledger.org
39. Enterprise Ethereum Alliance Advances Web 3.0 Era with Public Release of the Enterprise Ethereum Architecture Stack (May 2, 2018), located at https://entethalliance.org/enterprise-ethereum-alliance-advances-web-3-0-era-public-release-enterprise-ethereum-architecture-stack; https://entethalliance.org/wp-content/uploads/2018/05/EEA-TS-0001-0-v1.00-EEA-Enterprise-Ethereum-Specification-R1.pdf
40. Funk, Jeffrey L., Global Competition Between and Within Standards: The Case of Mobile Phones at 39 (New York, Palgrave, 2002); Garrard, Garry A., Cellular Communications: Worldwide Market Development (Boston, Artech House, 1998).
41. Gruber, Harald, The Economics of Mobile Telecommunications (Cambridge University Press, 2005) at 35.
42. *Id*.

* * *

Acknowledgment

The authors wish to thank Holland & Knight LLP partner, Joshua C. Krumholz, for his contributions to this chapter.

Ieuan G. Mahony
Tel: +1 617 573 5835 / Email: ieuan.mahony@hklaw.com

Ieuan G. Mahony is a partner in Holland & Knight's Boston office who concentrates his practice on intellectual property (IP) licensing and development, information technology (IT), and data privacy and security. Mr. Mahony combines his transactional and compliance work with dispute resolution and litigation matters. His substantial background in transactional and litigation practice areas helps clients receive high-quality advice in the dynamics of reaching an agreement as well as the realities of combating an adversary. Mr. Mahony is a member of the firm's three-partner Information Technology Governance Committee.

Brian J. Colandreo
Tel: +1 617 305 2143 / Email: brian.colandreo@hklaw.com

Brian J. Colandreo is a partner in Holland & Knight's Boston office. Mr. Colandreo serves as the National Patent Practice Leader. A registered patent attorney, Mr. Colandreo has considerable experience in many different aspects of intellectual property (IP) law. He represents (or has represented) foreign and domestic clients of all sizes – from sole inventors to Fortune 50 companies – in a wide range of technologies. *Intellectual Asset Management (IAM) Patent 1000* has recommended Mr. Colandreo since 2017. The publication states: "The 'excellent' Brian Colandreo is adored by clients. He's very bright and responsive. A lot of attorneys start with prosecution, but then get pulled into other things – not him, he loves it and you can see that in his work, which is a breath of fresh air."

Jacob Schneider
Tel: +1 617 305 2025 / Email: jacob.schneider@hklaw.com

Jacob Schneider is an intellectual property litigation partner whose practices focus on patent, trademark, copyright and trade secret litigation and licensing transactions. Mr. Schneider has substantial experience in a wide variety of technologies and industries, including telecommunications, transportation, computer hardware/software, web/mobile applications, blockchain, non-fungible tokens (NFTs), voice-recognition, sporting equipment, gaming, toys and life sciences devices. Mr. Schneider's educational and professional background is in computer software engineering and architecture, with a particular focus on web- and mobile-based applications.

Holland & Knight LLP

800 17th Street N.W., Suite 1100, Washington, D.C. 20006, USA
Tel: +1 202 955 3000 / Fax: +1 202 955 5564 / URL: www.hklaw.com

Cryptocurrency and other digital asset funds for U.S. investors

Gregory S. Rowland & Trevor Kiviat
Davis Polk & Wardwell LLP

Introduction

In 2008, an unknown author publishing under the name Satoshi Nakamoto released a white paper describing Bitcoin, a peer-to-peer version of electronic cash, and the corresponding software that facilitates online payments directly between counterparties without the need for a financial intermediary. In the nearly 15 years that have followed, Bitcoin and countless other open-source, decentralised protocols inspired by Bitcoin (for example, Ethereum and Litecoin) have come to represent a $1 trillion-plus market of alternative assets, commonly referred to as "digital assets", which are typically traded over the internet using online exchanges.

Digital assets can serve several functions. Although the following categories are not independent legal categories under U.S. law, such distinctions are helpful for understanding and crafting various investment strategies involving these assets. Some digital assets, such as Bitcoin or Litecoin, are widely regarded as decentralised stores of value or mediums of exchange due to certain common economic features that support these functions; these are sometimes referred to as "pure cryptocurrencies". Other digital assets, such as Monero or Zcash, are a subset of pure cryptocurrencies that also possess certain features designed to enhance transaction privacy and confidentiality ("privacy-focused coins").

Beyond pure cryptocurrencies and privacy-focused coins, there exists a broad array of general purpose digital assets ("platform coins"), such as Ethereum, Solana and Algorand, which are designed to facilitate various peer-to-peer activities, from decentralised software applications to "smart" contracts to digital collectibles, such as CryptoKitties, CryptoPunks and Bored Apes. Platform coins enable the creation of new digital assets called "tokens", which are typically developed for a specific purpose or application – for example: (1) "utility tokens", which generally are designed to have some consumptive utility within a broader platform or service; (2) "non-fungible tokens" or "NFTs", which are digital assets stamped with unique identifiers that enable creative applications like scarce digital art, trading cards and other collectibles; and (3) "security tokens", which are designed to represent more traditional interests like equity, debt and real estate with the added benefit of certain features of the digital asset markets, such as increased liquidity, more cost-effective fractional interest transfers, more efficient cross-border trading, faster and more transparent payment of dividends and other distributions and rapid settlement.

Finally, there is a category of digital assets called "stablecoins", which, as their name implies, are designed to offer 1:1 price stability by typically pegging their market value to an external reference asset, most commonly the U.S. Dollar. Platform coins and stablecoins provide the foundation for many of the protocols in the rapidly growing decentralised finance, or "DeFi", space.

The digital asset market extends beyond the assets themselves. Other participants, including online exchanges, payment processors and mining companies, compose the broader digital asset industry. And as this industry continues to grow, it has captured the attention of retail and institutional investors alike, including asset managers seeking to develop investment strategies and products involving these emerging assets and companies. Some strategies resemble early-stage growth strategies, featuring long-term investments either directly in certain digital assets or in start-up ventures developing complementary goods and services for the industry. Other strategies include hedge fund strategies, such as long/short funds, which often use derivatives, or arbitrage strategies, which seek to capitalise on the price fragmentation across the hundreds of global online exchanges. Additionally, during periods of weak or middling performance in the cryptocurrency markets – for example, during the so-called "crypto winter" of 2018–19 – fund managers began experimenting with novel revenue-generation strategies, such as staking cryptocurrencies,[1] adopting credit fund-type strategies (e.g., distressed debt), engaging in market-making and executing venture capital investments.[2]

This chapter outlines the current U.S. regulatory and tax framework applicable to cryptocurrency and other digital asset investment funds ("digital asset funds") offered to U.S. investors and how those regulatory and tax considerations affect fund-structuring decisions.

The U.S. regulatory framework generally

Digital asset funds operated in the United States or offered to U.S. investors must contend and comply with a complex array of federal statutes and regulations (in addition to state law, which is beyond the scope of this chapter). These include: the Securities Act of 1933 (the "Securities Act"), which regulates the offer and sale of securities; the Investment Company Act of 1940 (the "1940 Act"), which regulates pooled investment vehicles that invest in securities; the Commodity Exchange Act (the "CEA"), which regulates funds and advisers that trade in futures contracts, options on futures contracts, commodity options and swaps; and the Investment Advisers Act of 1940 (the "Advisers Act"), which governs investment advisers to such funds. Additionally, many fund-structuring decisions are driven by tax considerations. This section sets out the current U.S. federal regulatory framework applicable to digital asset funds managed in the United States or offered to U.S. investors and explores how those regulatory considerations affect fund-structuring decisions.

Offering of fund interests

Interests in investment funds are securities. Under the Securities Act, an offering of securities must be registered with the U.S. Securities and Exchange Commission (the "SEC") or made pursuant to an exemption. While there are a few possible exemptions, the most common exemption that private funds rely upon is Regulation D, which provides two alternative exemptions from registration: Rule 504 and Rule 506. Because most private investment funds intend to raise more than $5 million, Rule 506, which provides no limit on the amount of securities that may be sold or offered, is the exemption under Regulation D most commonly relied on by such funds, and consequently, this discussion of Regulation D is limited to offerings made under Rule 506.[3] In order to offer or sell securities in reliance on Rule 506 of Regulation D, an investment fund must:

- limit sales of its securities to no more than 35 non-accredited investors (unless the offering is made pursuant to Rule 506(c), in which case all purchasers must be accredited investors), although securities may be sold to an unlimited number of accredited investors;
- ensure that all non-accredited investors meet a sophistication requirement by having such knowledge and experience in financial and business matters that they are capable of evaluating the merits and risks of the prospective investment;

- refrain from general solicitation or advertising in offering or selling securities (unless the offering is made pursuant to Rule 506(c));
- comply with the information disclosure requirements of Rule 502(b) with respect to any offering to non-accredited investors. There are no specific information requirements for offerings to accredited investors;
- implement offering restrictions to prevent resales of any securities sold in reliance on Regulation D; and
- file a Form D notice of the offering with the SEC within 15 calendar days of the first sale of securities pursuant to Regulation D.

There are also some important limitations on the scope of the Regulation D exemption. For example, Regulation D only exempts the initial transaction itself (i.e., resales of securities acquired in an offering made pursuant to Regulation D must be either registered or resold pursuant to another exemption from registration). Furthermore, Regulation D is not available for any transaction or series of transactions that, while in technical compliance with Regulation D, is deemed to be part of "a plan or scheme to evade the registration provisions of the [Securities] Act".[4]

The regulatory treatment of cryptocurrencies and other digital assets

As discussed above, interests in investment funds themselves are securities; however, digital asset funds may hold a variety of different assets in pursuing their respective strategies – from digital assets themselves (e.g., Bitcoin and Ether) to derivatives instruments (e.g., Bitcoin futures contracts) to securities (e.g., equity in an emerging growth company or interests in another digital asset fund). This section provides an overview of the regulatory treatment of such assets, particularly with respect to the definitions of "securities" under the U.S. securities laws and "commodity interests" under the CEA, before explaining how these characterisations impact structuring decisions. Although some generalisations may be inferred about the possible treatment of certain assets based on common features and fact patterns, there is no substitute for a careful, case-by-case analysis of each asset, in close consultation with counsel.

In July 2017, in a release commonly referred to as the DAO Report,[5] the SEC determined that certain digital assets are securities for purposes of the U.S. federal securities laws. The DAO Report was published in response to a 2016 incident in which promoters of an unincorporated virtual organisation ("The DAO") conducted an initial coin offering ("ICO"), a term that generally refers to a sale of tokens to investors in order to fund the development of the platform or network in which such tokens will be used. The DAO was created by a German company called Slock.it, and it was designed to allow holders of DAO tokens to vote on projects that The DAO would fund, with any profits flowing to token-holders. Slock.it marketed The DAO as the first instance of a decentralised autonomous organisation, powered by smart contracts on a blockchain platform. The DAO's ICO raised approximately $150 million (USD) in Ether.

In the DAO Report, the SEC reasoned that The DAO tokens were unregistered securities because they were investment contracts, which is one type of security under the U.S. securities laws. Though it declined to take enforcement action against The DAO, the SEC used this opportunity to warn others engaged in similar ICO activities that an unregistered sale of digital assets can, depending on the facts and circumstances, be an illegal public offering of securities. The SEC has relied on similar reasoning in subsequent actions taken against token issuers that deem certain other digital assets sold in ICOs to be securities (such securities, "DAO-style tokens").[6] Many DAO-style tokens are branded by their promoters

as utility tokens to convey the idea that such tokens are designed to have some consumptive utility within a broader platform or service. However, as noted above, this terminology does not have any legal consequence under the U.S. securities laws. Instead, a proper inquiry must examine the facts and circumstances surrounding the digital asset's offering and sale, including the economic realities of the transaction.[7] Key factors to consider include: (1) whether a third party – be it a person, entity or coordinated group of actors – drives the expectation of a return; and (2) whether the digital asset, through contractual or other technical means, functions more like a consumer item and less like a security.[8] Additionally, in April 2019, the SEC staff published new detailed guidance on when a digital asset may be considered a security, in the form of two documents: a framework issued by the SEC's Strategic Hub for Innovation and Financial Technology along with a no-action letter from the SEC's Division of Corporation Finance. The framework reaffirms the staff's position that digital assets sold to investors to raise capital are generally securities, regardless of potential utility, and charts a narrow path for the sorts of digital assets that the staff would not consider a security. Meanwhile, the no-action letter is narrow and unlikely to provide meaningful guidance or practical utility for many types of currently available digital assets or firms considering issuing digital assets.[9] Finally, while it is beyond the scope of this chapter, the SEC has taken numerous enforcement actions against ICO issuers in cases where it believes that the offer and sale of the particular tokens in question amounted to an unregistered offering of securities.[10]

In addition to DAO-style tokens, some digital assets are explicitly designed to be treated as securities from the outset and are meant to represent traditional interests like equity and debt, with the added benefit of certain features of the digital asset markets, such as 24/7 operations, fractional ownership and rapid settlement. These digital assets are securities by definition, and although they represent an innovation in terms of how securities trade, clear and settle, they are not necessarily a new asset class.

Any cryptocurrencies or other digital assets that are not deemed to be securities under the U.S. securities laws may be considered "commodities" under the CEA, due to the broad definition of the term.[11] For example, the U.S. Commodity Futures Trading Commission (the "CFTC") appears to be treating Bitcoin as an exempt commodity under the CEA, a category that includes metals and energy products,[12] but does not include currencies or securities, which are classified as excluded commodities.[13] Additionally, in December 2017, the CFTC permitted the self-certification of futures contracts and binary options on Bitcoin by futures exchanges under its rules for listing ordinary futures contracts.[14] And although the SEC has not taken any action with respect to Bitcoin specifically, the SEC has informally acknowledged, and appeared to accept as correct, the CFTC's designation of Bitcoin as a commodity over which the CFTC has anti-fraud jurisdiction.[15] Finally, to the extent that a digital asset is a commodity, any derivatives offered on that commodity – for example, Bitcoin futures contracts and binary options – fall squarely within the definition of commodity interests under the CEA.

Possible obligations of the manager under the Advisers Act or the CEA

The question of whether a digital asset fund manager must comply with additional regulations under either, or both, the Advisers Act and the CEA turns primarily on the characterisation of the assets its funds hold. First, a manager is deemed an "investment adviser" under Section 202(a)(11) of the Advisers Act, and thus is subject to the rules and regulations thereunder, if it "for compensation, engages in the business of advising others, either directly or through publications or writings, as to the value of securities or as to the advisability of investing

in, purchasing, or selling securities", or "for compensation and as part of a regular business, issues or promulgates analyses or reports concerning securities". So, to the extent that a manager of a cryptocurrency or other digital asset fund is advising on "securities" – for example, because its funds hold DAO-style tokens or security tokens – it must register as an investment adviser with the SEC unless such individual or entity qualifies for an exclusion from the definition or an exemption from the registration requirement.[16]

Registration under the Advisers Act subjects advisers to a host of rules and regulations, including those governing advertising, custody, proxy voting, record-keeping, the content of advisory contracts and fees. For example, the Advisers Act custody rule[17] (the "custody rule") has detailed provisions applicable to any SEC-registered investment adviser deemed to have custody, as defined under the rule. Among other requirements, it requires use of a "qualified custodian" to hold client funds or securities, notices to clients detailing how their assets are being held, account statements for clients detailing their holdings, annual surprise examinations and additional protections when a related qualified custodian is used. For example, investment advisers dealing in digital assets may need to consider whether a bank, registered broker-dealer or other firm that meets the definition of a qualified custodian, is willing to take custody of the digital assets.

Second, managers of private funds that invest or trade in "commodity interests", whether as an integral part of their investment strategy or only in a limited capacity, for hedging purposes or otherwise, are subject to regulation under the CEA and the rules of the CFTC thereunder (the "CFTC Rules"). Commodity interests generally include: (1) futures contracts and options on futures contracts; (2) swaps; (3) certain retail foreign currency and commodity transactions; and (4) commodity options and certain leveraged transactions. So, to the extent that the activities of a manager of a cryptocurrency or other digital asset fund include trading in commodity interests – for example, because it holds Bitcoin futures contracts or binary options – it will be subject to registration and regulation as a commodity pool operator ("CPO") or commodity trading advisor ("CTA"), unless it qualifies for an exemption or exclusion under the CEA or the CFTC Rules.

If the activities of an investment fund bring it within the definition of a "commodity pool" under the CEA, the manager of the fund is required to register as a CPO with the CFTC, unless such person otherwise qualifies for an exclusion from the definition of CPO or an exemption from the registration requirement. The CEA also provides for the registration of CTAs, which is in some respects analogous to the treatment of investment advisers under the Advisers Act. It should be noted, however, that numerous requirements under the CEA and the CFTC Rules apply to all CPOs and CTAs, even those that are exempt from registration.

Possible obligations of the fund under the 1940 Act or the CEA

Similarly, the fund itself may be subject to additional regulations under either, or both, the 1940 Act and the CEA, an analysis that, again, turns primarily on the assets the fund holds. An investment company is defined under Section 3(a)(1)(A) of the 1940 Act as any issuer that "is or holds itself out as being engaged primarily, or proposes to engage primarily, in the business of investing, reinvesting or trading in securities". This subjective test is based generally on how a company holds itself out to the public and the manner in which it pursues its business goals, and is designed to capture traditional investment companies that are deliberately acting in that capacity. Additionally, Section 3(a)(1)(C) of the 1940 Act sets forth an objective, numerical test that applies to companies that hold a significant portion of their assets in investment securities, even if they do not hold themselves out as traditional investment companies.

Companies that fall within one of these definitions of an investment company must either satisfy an exemption from the 1940 Act or register under it. The 1940 Act is a comprehensive statutory regime that imposes strict requirements on registered investment companies' governance, leverage, capital structure and operations. Consequently, most private equity funds, hedge funds and other alternative investment vehicles, which fall squarely within the definition of "investment company", are structured to satisfy an exemption from the 1940 Act.

The 1940 Act provides specific exemptions from the definition of "investment company" for privately offered investment funds and certain other types of companies. For example, Section 3(c)(1) exempts a private investment fund from registration if the outstanding securities of such fund (other than short-term paper) are beneficially owned by not more than 100 persons and such fund does not presently propose to make a public offering of its securities. Further, Section 3(c)(7) exempts a private investment fund from registration if all of the beneficial owners of its outstanding securities are "qualified purchasers" and the entity does not make or propose to make a public offering of its securities, and it does not limit the number of beneficial owners.

The CEA defines "commodity pool" as any investment trust, syndicate or similar form of enterprise operated for the purpose of trading in commodity interests. The CFTC interprets "for the purpose" broadly and has rejected suggestions that trading commodity interests must be a vehicle's principal or primary purpose. As a result, any trading by a private fund in swaps, futures contracts or other commodity interests, no matter how limited in scope, and regardless of whether undertaken for hedging or speculative purposes, generally will bring a private fund within the commodity pool definition.

According to the CFTC, a fund that does not trade commodity interests directly but invests in another fund that trades commodity interests would itself be a commodity pool. Thus, in a master-feeder fund structure, a feeder fund will be considered a commodity pool if the master fund is a commodity pool. Similarly, a fund of funds that invests in commodity pools may itself be considered a commodity pool.

Finally, an investment vehicle can be both an "investment company" under the 1940 Act and a "commodity pool" under the CEA, and an exemption from the registration requirements of the 1940 Act does not generally imply an exemption from CPO registration under the CEA (or *vice versa*). Similarly, an exemption from registration under the Advisers Act does not generally imply an exemption from CTA registration (or *vice versa*). Furthermore, interests in commodity pools are "securities" under the Securities Act, and therefore the Securities Act applies to the offer and sale of interests in a commodity pool to the same extent as it applies to any other type of security. Accordingly, offering of interests in a private fund that is a commodity pool generally will be structured to meet the requirements of a Securities Act exemption (e.g., Regulation D, as discussed above).

Applying this framework to digital asset funds

Given the regulatory minefield laid out above, managers face a multitude of structuring decisions in conceiving, launching and operating digital asset funds aimed at U.S. investors. These decisions will often influence, and be influenced by, the manager's investment strategy – particularly as it relates to the types of assets the fund should be permitted to hold. This section explores some common structures and the strategies they support. In each of these cases, one should keep in mind that interests in the digital asset fund itself are securities, as noted above, that must be offered and sold pursuant to an exemption, such as Regulation D, except in the case of registered (i.e., public) funds, which are offered and sold in fully registered securities offerings.

First, the manager may decide that the fund should have flexibility to invest in securities. It may want to invest in "traditional" securities like equity or debt in a company within the digital asset industry (including through tokenised securities), or DAO-style tokens and other digital assets at risk of being deemed investment contracts. In this case, the adviser will likely need to register under the Advisers Act and comply with the host of rules and regulations thereunder, including those governing advertising, custody, proxy voting, record-keeping, the content of advisory contracts, and fees. Non-U.S. advisers, however, can potentially rely on Advisers Act Rule 203(m)-1 (the "private fund adviser rule").[18]

Custody poses unique questions in the digital asset context, and it is not clear in all cases whether digital assets would be viewed as funds or securities, such that the custody rule would apply. Currently, most qualified custodians do not offer custody services for digital assets. In any case, the manager should familiarise itself with the operational considerations of digital asset custody. First, what does it mean to have custody of an asset that is not physical and, even in digital form, does not exist on a centralised database, but instead on one that is universal and distributed? For example, one cannot physically move units of Bitcoin off of the Bitcoin blockchain and store them elsewhere. However, in order to exercise control over one's Bitcoins, one needs a private and a public key. These keys are a series of hexadecimal characters (e.g., 1A1zP1eP5QGefi2DMPTfTL5SLmv7DivfNa), which must be stored carefully. The public key is the identity of the address on the network that has ownership and control of those Bitcoins – this key can be shared with anyone, and in fact, it must be shared in order to receive Bitcoins. The private key is essentially a password, and Bitcoins can be transferred out of a particular address by anyone with possession of that address's corresponding private key. So, in the case of a blockchain-based asset like Bitcoin, control of the private key may be tantamount to custody. As there is simply no recourse to retrieve Bitcoins when a private key is lost or stolen, a critical operational point for managers is safe and secure private key storage; for example, through "deep cold" storage.[19]

If the manager believes the digital asset fund may invest in securities, the fund itself would likely be structured so as to meet one of the various registration exemptions for entities that would otherwise be classified as "investment companies" under the 1940 Act.[20] For offshore funds, the requirements of Sections 3(c)(1) and 3(c)(7), which are discussed above, generally only apply to U.S. investors.

Alternatively, the manager may consider structuring the fund as a registered investment company. As of the date of this chapter, the SEC has not approved any such funds that invest directly in digital assets, but has permitted exchange-traded funds and other registered funds to invest in certain Bitcoin futures contracts.[21] In considering these issues, the SEC's Division of Investment Management has outlined several questions that sponsors would be expected to address before it would consider granting approval for funds holding "substantial amounts" of cryptocurrencies or "cryptocurrency-related products".[22] The questions, which focus on specific requirements of the 1940 Act, generally fall into one of five key areas: valuation; liquidity; custody; arbitrage; and potential manipulation. And although such funds alternatively could potentially be offered to the public as non-investment companies (to the extent they do not hold significant amounts of securities) under the Securities Act, the SEC has indicated that significant, similar questions exist there also.[23]

Second, the manager may decide that the fund should have flexibility to invest in commodity interests, such as futures contracts or binary options, either for hedging or speculative purposes. Any such trading by a private fund, no matter how limited in scope, and regardless of the purpose, would generally make such fund a "commodity pool", as discussed above. In

this case, the manager may be required to register as a CPO or CTA with the CFTC, although certain exemptions exist for non-U.S. managers and for funds that invest in only limited amounts of commodity interests. Even if the manager decides that such fund should only invest in commodity interests and not securities, interests in commodity pools are "securities" under the Securities Act, and therefore, the fund would generally be structured to meet the requirements of a Securities Act exemption (e.g., Regulation D, as discussed above).

Finally, the manager may decide that the fund should hold neither securities nor commodity interests – in other words, a fund that holds only commodities, or "pure cryptocurrencies", such as Bitcoin, and no commodity interests. Because this category does not have independent legal significance under U.S. law, such determinations regarding the risk that a given digital asset could be deemed a "security" for U.S. securities laws purposes should be made carefully and together with counsel. In this case, the fund would not be governed by the 1940 Act, and the manager's activities with respect to the fund would not be governed by the Advisers Act, as both of these regimes are premised upon the fund holding securities, as discussed above. Further, because the fund does not hold commodity interests, it would likely not be considered a "commodity pool", and the manager would likely not be required to register as a CPO or CTA with the CFTC. However, the fund and the manager in this case would not be entirely unregulated. As noted above, interests in the fund are securities (regardless of the underlying assets that the fund invests in), the offer and sale of which must comply with U.S. securities laws. Additionally, the CFTC has some, albeit limited, jurisdiction over the spot market for commodities pursuant to its anti-fraud and manipulation authority.[24] Moreover, the manager of such a fund would likely be considered a common law fiduciary to such a fund and thus subject to fiduciary duties in its management of the fund.

U.S. federal income tax framework

Tax considerations are often a principal driver for managers when deciding how to structure an investment fund. For managers of funds that invest in or trade digital assets, these structuring decisions are particularly complex given the limited guidance and uncertainty that exist with respect to the treatment of digital assets for U.S. federal income tax purposes.

The U.S. federal income tax treatment of cryptocurrencies and other digital assets

Through three pieces of published guidance, the U.S. Internal Revenue Service (the "IRS") has established a limited framework for analysing the U.S. federal income tax consequences of digital asset transactions. In Notice 2014-21,[25] the IRS established that "virtual currency", defined as a "digital representation of value that functions as a medium of exchange, a unit of account, and/or a store of value", is treated as "property" that is not "currency" and, therefore, that general tax principles applicable to property transactions apply to transactions using virtual currency. Thus, for example, assuming that a taxpayer holds a unit of virtual currency as a capital asset (which includes property held for investment purposes), a disposition of that virtual currency will result in capital gain or loss to the taxpayer. In 2019, the IRS simultaneously released a revenue ruling[26] and a series of "frequently asked questions"[27] (the "Ruling & FAQs") that provide additional guidance with respect to the taxation of virtual currency. The Ruling & FAQs establish the IRS's position that a hard fork of virtual currency will give rise to taxable ordinary income equal to the fair market value of the new virtual currency that arises as a result of the fork if a taxpayer is able to exercise "dominion and control" over that new virtual currency,[28] and provide guidance on a number of other ancillary issues relevant to the taxation of virtual currency (including matters relating to basis, holding period and certain other tax accounting issues).

Despite this guidance, there are many aspects of the taxation of digital assets that remain unclear, including issues that are of particular import to fund managers when considering how to efficiently structure a fund that invests in or trades digital assets. These areas of uncertainty include whether: (i) income and gain from digital assets constitutes, for instance, "qualifying income" for purposes of the publicly traded partnership rules, or "passive income" for purposes of the "passive foreign investment company" (or "PFIC") rules; (ii) staking rewards or income from forks, airdrops or similar occurrences ("fork-type income") constitutes "unrelated business taxable income" (or "UBTI") for U.S. tax-exempt investors; (iii) buying and selling digital assets might rise to the level of a trade or business in the United States, such that income from such activities constitutes income that is treated as effectively connected with a trade or business in the United States ("effectively connected income"); (iv) engaging in staking activities, either directly or via a third-party validator, might rise to the level of a trade or business in the United States, such that income from such activities constitutes effectively connected income; (v) any or all digital assets are considered "commodities" for certain purposes under the U.S. Internal Revenue Code of 1986, as amended (the "Code"); (vi) staking rewards or fork-type income is subject to non-resident alien tax withholding;[29] and (vii) whether a loan of digital assets is a taxable event.[30]

Applying this framework to digital asset funds

Many private investment fund structures consist of at least two vehicles: a vehicle that is treated as a partnership for U.S. federal income tax purposes (a "Master Fund"); and a vehicle that invests all or substantially all of its funds in the Master Fund, is organised in a non-U.S. jurisdiction[31] and is treated as a corporation for U.S. federal income tax purposes (an "Offshore Fund"). U.S. taxable investors generally invest (directly or through other partnership fund vehicles) in the Master Fund, and, because partnerships receive "pass-through" treatment for U.S. tax purposes, the U.S. investors generally are treated as if they directly derived their shares of the Master Fund's items of taxable income, gains, losses and deductions. Non-U.S. and U.S. tax-exempt investors generally invest in the Offshore Fund in order to "block" certain types of income that could cause adverse tax consequences to those investors if received directly. Other investment fund structures utilise a single partnership or corporate vehicle. The choice of fund structure for a digital asset investment vehicle may be informed by the manager's investment strategy and the composition of the vehicle's investor base.

As noted above, many private investment funds include a Master Fund designed to be treated as a partnership for tax purposes. In that regard, the "publicly traded partnership" rules of the Code provide that if interests in a partnership are traded on an established securities market or are readily tradable on a secondary market, a test that takes into account whether partnership units are redeemable on a frequent basis, the partnership generally will be treated as a corporation for U.S. federal income tax purposes, unless at least 90% of the partnership's income for each taxable year consists of "qualifying income".[32] While there are strong arguments, both based on the statutory text of Section 7704 of the Code (as well as the relevant Treasury Regulations) and from a tax policy perspective, for treating income and gains from investments in digital assets and from certain types of staking activities as "qualifying income", the lack of guidance on this issue has left fund managers facing a trade-off between the tax efficiency of a pass-through vehicle and liquidity for investors. To ensure that the Master Fund does not become subject to corporate-level U.S. tax (or treatment as a PFIC), managers often restrict the number of persons that may invest in the fund or the frequency with which investors are able to transfer or redeem their interests.

Where a partnership is used as a digital asset investment vehicle, the use of an offshore "blocker" corporation might be necessary to attract non-U.S. and tax-exempt investors. In particular, although there is a statutory safe harbour for investment vehicles that trade in commodities and securities, there is uncertainty regarding whether any or all digital assets qualify as commodities (or securities) that are within the purview of this safe harbour and whether a fund's transactions in them meet the other requirements of the trading safe harbour. Other common activities (e.g., relating to staking) conceivably might constitute a trade or business in the United States. Moreover, uncertainty regarding whether fork-type income and staking rewards constitute UBTI could cause U.S. tax-exempt investors to favour holding any investments in digital assets through a "blocker" corporation.[33]

In addition to using non-U.S. corporations as "blockers", managers that seek to offer greater liquidity in their digital asset funds than might be available through a partnership structure (because of the reasons described above) sometimes offer interests in a non-U.S. corporate investment vehicle to taxable U.S. investors. However, the consequences to a taxable U.S. investor of investing in such vehicles are also subject to some uncertainty. In particular, the IRS's position in the Ruling & FAQs that a hard fork of virtual currency can give rise to taxable income suggests that such funds might not be PFICs, but this is unclear.[34] Classification as a PFIC can result in significant administrative and reporting burdens for the corporation and its shareholders and, absent certain elections, U.S. shareholders in a PFIC are generally subject to disadvantageous tax consequences.

The preceding discussion addresses but a few of the myriad structuring and other tax considerations implicated by investments in digital assets, others of which are similarly subject to uncertainty given the nascent state of guidance in the area. As the tax law applicable to investments in digital assets continues to develop, managers and their advisors must carefully consider and plan for these issues.

Conclusion

Over the past decade, digital assets have come a long way – from Satoshi's original Bitcoin white paper to today's broad universe of countless digital assets trading across hundreds of online trading venues. As this market and the surrounding industry matures, asset managers will likely continue to identify opportunities to either deploy novel investment strategies or adapt their tried-and-true strategies in this new context. As set out above, such managers face a complex array of statutes and regulations in offering digital asset funds to U.S. investors and optimising their funds' tax characteristics. These considerations, together with the investment strategies that the manager desires to pursue, affect fund-structuring decisions, and accordingly, are best addressed together with counsel.

* * *

Endnotes

1. Proof of Stake – Bitcoin Wiki, https://en.bitcoin.it/wiki/Proof_of_Stake (last visited Jul. 26, 2023) (staking involves users locking tokens in a wallet that is then used to secure the network, validate transactions and produce new blocks, thereby allowing users to earn a passive income return). These additional activities, such as market-making, may raise additional U.S. regulatory issues that are beyond the scope of this chapter.
2. Frank Chaparro, Crypto hedge funds are getting creative as the bear market tightens its grip, The Block (2018), https://www.theblockcrypto.com/2018/12/04/crypto-

hedge-funds-are-getting-creative-as-the-bear-market-continues-to-grip-crypto/ (last visited Jul. 26, 2023).

3. Historically, issuers and any persons acting on their behalf were prohibited from engaging in any form of general solicitation or general advertising in Rule 506 offerings. However, in July 2013, the SEC adopted final rules to permit general solicitation and general advertising in Rule 506 offerings under new Rule 506(c). Additional requirements apply to Rule 506(c) offerings, including the requirement to take reasonable steps to verify an investor's accredited investor status. Under Rule 506(b), an investment fund may offer securities pursuant to Rule 506 without complying with these additional requirements if it does not use general solicitation. Currently, most private funds offered in the United States choose not to use general solicitation.
4. *See* 17 CFR 230.500(f).
5. SEC Release No. 81207, *Report of Investigation Pursuant to Section 21(a) of the Securities Exchange Act of 1934: The DAO* (Jul. 25, 2017).
6. *See*, *e.g.*, SEC Release No. 10445, *In the matter of Munchee, Inc.* (Dec. 11, 2017).
7. This includes, for example, (1) whether the investor's fortunes are interwoven with those of other investors or the efforts of the promoter of the investment, and (2) whether the investor's expectation of profits are based predominantly upon the entrepreneurial or managerial efforts of the promoter or other third parties. *See SEC v. W.J. Howey Co.*, 328 U.S. 293, 301 (1946).
8. Director William Hinman, Remarks at the Yahoo Finance All Markets Summit, *Asset Transactions: When Howey Met Gary (Plastic)* (Jun. 14, 2018), available at https://www.sec.gov/news/speech/speech-hinman-061418. Further, the speech indicates that a digital asset that was originally offered in a securities offering may later be sold in a manner that does not constitute an offering of a security, in limited circumstances, where: (i) there is no longer a central enterprise being invested in; and (ii) the asset is only being sold to end users who will purchase a good or service available through a network. This also raises a counterfactual question – that is, whether a token network that was once decentralised could "centralise", such that it would fall within the scope of the securities laws even though it had previously not been a security. For example, fundamental changes to a given token network could cause the SEC staff and certain market participants to revisit the securities law analysis for the associated token.
9. SEC, Staff Guidance: Framework for "Investment Contract" Analysis of Digital Assets (Apr. 3, 2019), available at https://www.sec.gov/corpfin/framework-investment-contract-analysis-digital-assets (the "Framework"). SEC, No-Action Letter: Response of the Division of Corporation Finance Re: TurnKey Jet, Inc. (Apr. 3, 2019), available at https://www.sec.gov/divisions/corpfin/cf-noaction/2019/turnkey-jet-040219-2a1.htm (the "No-Action Letter").
10. *See*, *e.g.*, SEC, Press Release: Telegram to Return $1.2 Billion to Investors and Pay $18.5 Million Penalty to Settle SEC Charges (Jun. 26, 2020), available at https://www.sec.gov/news/press-release/2020-146
11. *See* 7 U.S.C. § 1a(9).
12. *See* 7 U.S.C. § 1a(20) (defining exempt commodity to mean any commodity that is not an agricultural commodity or an excluded commodity; excluded commodity is defined in Section 1a(19) of the CEA to include any "interest rate, exchange rate, currency, security, security index" and other financial rates and assets).
13. *See In re Coinflip, Inc.*, CFTC No. 15-29, 2015 WL 5535736 (Sept. 17, 2015). In this order, the CFTC found that Coinflip's Bitcoin options were offered in violation of CFTC Regulation 32.2, which governs commodity option transactions. The CFTC

noted that the options "were not conducted pursuant to [CFTC] Regulation 32.3", the so-called "trade option exemption", which permits trading of commodity options on exempt and agricultural commodities, but not on excluded commodities such as securities, currencies, interest rates and financial indices. The CFTC, in describing why the trade option exemption was not available for Coinflip's options, focused on requirements under CFTC regulation that the options must be offered by eligible contract participants to commercial users of the underlying commodity, and not on the classification of Bitcoin as an excluded commodity.

14. *See* CFTC Release pr7654-17, CFTC Statement on Self-Certification of Bitcoin Products by CME, CFE and Cantor Exchange (Dec. 1, 2017). *See also* CFTC Backgrounder on Oversight of and Approach to Virtual Currency Futures Markets (Jan. 4, 2018) (describing the CFTC's authority with respect to virtual currency and the "heightened review" employed during the Bitcoin futures self-certification process).
15. Then-SEC Chairman Jay Clayton, Statement on Cryptocurrencies and Initial Coin Offerings, at n. 2 (Dec. 11, 2017) ("The CFTC has designated Bitcoin as a commodity. Fraud and manipulation involving Bitcoin traded in interstate commerce are appropriately within the purview of the CFTC, as is the regulation of commodity futures tied directly to [B]itcoin."); *see also* CNBC, *SEC Chief Says Agency Won't Change Securities Laws to Cater to Cryptocurrencies* (Jun. 6, 2018) ("'Cryptocurrencies: These are replacements for sovereign currencies, replace the dollar, the euro, the yen with [B]itcoin,' Clayton said. 'That type of currency is not a security.'").
16. Investment advisers not registered with the SEC may be subject to registration with U.S. states.
17. 17 U.S.C. § 206(4)-2.
18. For an adviser that has its principal office and place of business outside of the United States, an Advisers Act registration exemption is available under the private fund adviser rule, so long as: (i) the adviser has no client that is a U.S. person (generally as defined in Regulation S under the Securities Act) except for "qualifying private funds" (as defined in the rule); and (ii) all assets managed by the adviser at a place of business in the United States are solely attributable to private fund assets with a value of less than $150 million. Advisers relying on this exemption are still required to file certain information with the SEC.
19. Cold storage refers to the process of storing digital assets, such as Bitcoins, offline (i.e., storing the private keys on a device not connected to the internet). However, the private keys associated with this process may have been exposed to the internet at some time during the generation of the signing process. Deep cold storage, however, is a type of cold storage where not only are the digital assets stored offline, but also the private keys associated with those assets are generated in offline systems, and the signing process of the transactions is also made in offline systems. The systems used in this type of storage never touch the internet; they are created offline, they are stored offline, and they are offline when signing transactions.
20. *See* 1940 Act § 3(c)(1)-(7).
21. *See* Division of Investment Management Staff Statement on Funds Registered under the Investment Company Act Investing in the Bitcoin Futures Market (available at https://www.sec.gov/news/public-statement/staff-statement-investing-bitcoin-futures-market). The staff noted that, among open-end funds, it "believes at this time that investment in the Bitcoin futures market should be pursued only by mutual funds with appropriate strategies that support this type of investment and full disclosure of material risks". *See*

also SEC Chairman Gary Gensler, Remarks Before the Aspen Security Forum (Aug. 3, 2021) ("I anticipate that there will be filings with regard to exchange-traded funds under the Investment Company Act. When combined with the other federal securities laws, the '40 act provides significant investor protections. Given these important protections, I look forward to the staff's review of such filings, particularly if those are limited to these CME-traded Bitcoin futures."). The first U.S. exchange-traded fund investing in Bitcoin futures began trading on October 19, 2021. Even more recently, the SEC permitted the public offering of exchange-traded funds that invest in Bitcoin futures but are not registered as investment companies under the 1940 Act. Given the additional regulatory burdens imposed by the 1940 Act, a fund sponsor may find this more recent form of Bitcoin futures exchange-traded fund preferable.

22. SEC, Staff Letter: Engaging on Fund Innovation and Cryptocurrency-related Holdings (Jan. 18, 2018), available at https://www.sec.gov/divisions/investment/noaction/2018/cryptocurrency-011818.htm (the "Letter").
23. *See*, *e.g.*, SEC Release No. 34-87267; File No. SR-NYSEArca-2019-01 (Oct. 9, 2019), https://www.sec.gov/rules/sro/nysearca/2019/34-87267.pdf (last visited Jul. 26, 2023).
24. *See* CFTC Rule 180.1.
25. 2014-1 C.B. 938.
26. Rev. Rul. 2019-24, 2019-44 I.R.B. 1044. *See also* IRS Chief Counsel Advice Memorandum 202114020 (April 9, 2021) (holding that a taxpayer who received Bitcoin Cash as a result of the August 1, 2017 Bitcoin hard fork was required to recognise income when the taxpayer obtained dominion and control over the Bitcoin Cash).
27. Available at https://www.irs.gov/individuals/international-taxpayers/frequently-asked-questions-on-virtual-currency-transactions. Positions expressed in "FAQs" published by the IRS are not binding authority and may not be cited as precedent in litigation. However, the positions taken in FAQs are helpful because they demonstrate the reasoned views of the IRS with respect to the issues discussed therein.
28. Notwithstanding this seemingly straightforward proposition, the analysis set forth in Revenue Ruling 2019-24 has created confusion among market participants because it refers to "hard forks" and "airdrops" in a manner that does not track those terms' usage in common industry parlance. Thus, the exact scope of the holdings of Revenue Ruling 2019-24 remains unclear.
29. Under current law, it is not clear whether fork-type income or income from staking is U.S.- or foreign-source income, or whether it constitutes "fixed or determinable annual or periodical income" (or "FDAP"). Withholding agents, which can include investment vehicles (both partnerships and corporations), are generally required to withhold on and report payments of U.S.-source FDAP to non-resident aliens. The source and character of income can otherwise affect the reporting and withholding obligations of withholding agents as well.
30. Managers may seek to organise funds that are permitted to make loans of digital assets held by the fund in order to generate additional returns for investors in the form of loan fees and interest. While many digital asset loans resemble market-standard security loans, which generally qualify for the non-recognition provision of Section 1058 of the Code (as defined above), it is unclear whether a lender will recognise gain or loss as a consequence of entering into a digital asset loan or as a consequence of the receipt of digital assets upon the termination of a digital asset loan because Section 1058 applies only to loans of securities (including corporate stock). Despite the existence of strong policy arguments in favour of non-recognition treatment for

digital asset loans that resemble market-standard security loans, the risk of triggering taxable gain looms as a possible deterrent to lending activities for funds that are U.S. tax-sensitive.

31. Managers often seek to organise their Offshore Funds or other non-U.S. corporate vehicles in jurisdictions with favourable tax regimes, such as the Cayman Islands or the British Virgin Islands.
32. "Qualifying income" can include income and gain from commodities and income "substantially similar" to income from "ordinary and routine investments to the extent determined by the Commissioner". *See* IRC § 7704; Treas. Reg. § 1.7704-3.
33. Section 511 of the Code taxes UBTI received by U.S. tax-exempt entities at the rates applicable to corporations or trusts, depending on the relevant entity's tax classification.
34. If 75% or more of the income of a non-U.S. corporation consists of "passive income", or if 50% or more (by value) of its assets are "passive assets", that corporation generally will be treated as a PFIC. *See* IRC § 1297(a). For purposes of the PFIC rules, "passive assets" include assets that do not produce income, and "passive income" includes gain from the sale of passive assets. *See* IRC §§ 1297(a), (b); 954(c)(1)(B)(iii). "Passive income" also includes the excess of gains over losses from transactions in any "commodities" (as defined for purposes of Section 954 of the Code), and therefore any "commodity" as so defined would automatically be a "passive asset". *See* IRC §§ 1297(a), (b); 954(c)(1)(C). Strong arguments exist for treating certain digital assets as "commodities" for purposes of various Code sections, including Section 954, but this aspect of the taxation of digital assets is likewise uncertain.

* * *

Acknowledgments

The authors gratefully acknowledge Patrick E. Sigmon, a Partner in Davis Polk's Tax Department, and Joel Kuzniecky, an Associate in Davis Polk's Investment Management Group, for their assistance in the preparation of this chapter.

Gregory S. Rowland
Tel: +1 212 450 4930 / Email: gregory.rowland@davispolk.com

Gregory S. Rowland is a Partner in Davis Polk's Corporate Department, practising in the Investment Management Group. He focuses on providing transactional, regulatory and compliance advice relating to investment advisers, mutual funds, closed-end funds, business development companies, private equity funds and hedge funds. He devotes a large portion of his practice to the structuring, launch and operation of registered investment companies and hedge funds and to the sales, acquisitions and restructurings of asset management firms.

Mr Rowland advises financial institutions, technology companies and asset managers in connection with transactional, regulatory and compliance issues concerning digital currency and blockchain activities, including digital currency fund formation. In addition, he advises financial institutions, fund sponsors, corporations, employees' securities companies, and other entities regarding exemptions under the Investment Company Act and Investment Advisers Act.

Trevor Kiviat
Tel: +1 212 970 8194 / Email: trevor.kiviat@nydig.com

Trevor Kiviat is Senior Counsel at New York Digital Investment Group LLC ("NYDIG"), where he works on novel strategic, operational and legal issues relating to digital currency-based businesses. Prior to NYDIG, Mr Kiviat was an Associate at Davis Polk, where his practice focused on advising clients on the formation and operation of private investment funds, including private equity funds, hedge funds and venture capital funds.

In addition, Mr Kiviat wrote the first widely read and cited academic paper discussing Bitcoin and blockchain policy frameworks. He has been cited in the media for his extensive knowledge in this area and has lectured on related topics at the International Monetary Fund, Duke University and Georgetown University.

Davis Polk & Wardwell LLP

450 Lexington Avenue, New York, NY 10017, USA
Tel: +1 212 450 4000 / URL: www.davispolk.com

Layer-2 sequencing demystified: A lawyer's introduction

Angela Angelovska-Wilson & Tom Momberg, DLx Law
Michael Mosier, Arktouros PLLC

Introduction

The most popular "layer-1" blockchain networks, like Ethereum, have long suffered from limitations on scalability. In recent years, so-called "layer-2 rollups," which are distinct blockchain networks that run protocols to bundle (or "roll up") hundreds of separate individual "database transactions"[1] into a single entry on the layer-1 network (often called the "mainnet"), have emerged as the leading solution to these challenges.[2]

Rollups – by processing the majority of transactions on a separate "layer-2" blockchain network (*i.e.*, off the mainnet) and only committing a concise summary of those database transactions to the layer-1 chain – significantly enhance the main network's transactional throughput.[3] This ensures that the mainnet remains responsive and adaptable to increasing computational demands and growing network activity.[4]

Central to a rollup's operation is the "sequencer," a mechanism designed to determine the canonical order of database transactions.[5] A sequencer's primary function is simply to decide the order of transactions, but this makes it essential for supporting web3 infrastructure's reliability, efficiency, and consistency. Given the operational complexity of these functions, we attempt in this chapter to distill the fundamentals, so as to help prevent misunderstandings and misapplication of wrongly "analogous" legal constructs on neutral data and communications infrastructure by lawyers or policymakers.[6]

Crucially, a sequencer, like any other element of a layer-2 blockchain protocol, does not inherently introduce functionalities that could be broadly understood as providing regulatorily sensitive products or services. Rather, the sequencer is a technological component of a broader software-based framework that provides for greater and more efficient functionality on the underlying layer-1 blockchain.[7] A sequencer's primary objective is to algorithmically interpret incoming transaction data and output ordered blocks, thereby optimizing a blockchain system's throughput and efficiency.[8]

Although technically complex, the role of sequencer functionality is not particularly novel. Just like technology providers in traditional data infrastructures, sequencers are no more than an objective[9] software program being run to provide a purely technological service, with no intended ability to include independent discretion, judgment, or input.[10] This chapter examines the intricacies of the technical solutions that sequencers seek to offer and calls for collaboration and understanding to assist both lawyers and developers seeking to understand and bolster the integrity of layer-2 blockchain systems.

Redefining data infrastructure: Bridging tech and legal frontiers

In contrast with open, blockchain-based networks, most current data infrastructures are generally opaque to the public, managed by dominant and concentrated data infrastructure

providers.[11] These systems undergo significant downtime and rely on intermediaries, each, a single point of failure. Conventional data infrastructure is also prone to the influence of political aims and the powers of the largest providers of capital, which can favor or disfavor various economic sectors, geographies, or groups of persons or organizations.

Blockchain technology, including layer-2 rollup functionality, differs from the traditional approach because it offers a transparent, distributed ledger where publicly accessible data accompanies each transaction. This transparency and much higher level of decentralization mean that most of the potential risks or harms necessitating licensed intermediaries in traditional systems are inherently addressed.[12]

The architecture of traditional data systems is highly centralized, with few globally dominant data infrastructure providers wielding the vast majority of control over all data and systems.[13] This centralization can lead to its own inefficiencies and vulnerabilities, as well as a lack of transparency.[14] To the contrary, the decentralized nature of blockchain networks significantly reduces, if not eliminates, any opportunity for a single person or group to assume undue control over the network, promoting transparency, security, and efficiency. Database transactions made on blockchain networks are verifiable, irreversible (within the bounds of the protocol), and can be viewed by anyone. The order of transactions and state of the blockchain can also always be challenged, ensuring accountability and reducing the potential for many traditional forms of fraudulent activities.

As layer-2 rollup protocols evolve and become increasingly common, and as this allows the use of blockchain and digital assets to scale, this technology demands a comprehensive understanding – not just by the developers who are building with it, but also – by professionals in law, risk, compliance, and policy. It is no longer sufficient for lawyers, courts, policymakers, and other stakeholders to maintain a mere "general understanding" of these technologies. Given blockchain technology's continuing evolution and the increasing complexity of the solutions this technology entails, stakeholders must familiarize themselves with the nuances of these technologies and their practical implications before taking action that could substantially impact this area of innovation.[15] Only with a thorough grasp of the details can these professionals embark on a meaningful analysis or draw informed conclusions about layer-2 sequencing's role in the blockchain ecosystem or any potentially regulated or controlled activities.

Technical foundations of layer-2 sequencing

Ethereum's expanding user base has accentuated the network's throughput capacity limitations, underscoring the urgency for scalable solutions. The essence of scalability lies in amplifying speed and throughput without sacrificing the pillars of decentralization or security.[16] On the Ethereum mainnet, surges in demand at any given time can decelerate validation of pending database transactions and inflate gas[17] prices, emphasizing the need to bolster network capacity for Ethereum's widespread adoption.[18]

Layer-2 rollups

Layer-2 rollups stand at the forefront of solutions addressing the scalability challenges inherent in blockchain networks, especially Ethereum.[19] These rollups leverage cryptographic and mechanism design techniques to allow transactions to be batched before being posted to the layer-1 blockchain, optimizing database transaction costs for blockchain users.[20]

Technically, a "rollup" is a function that is applied to input array data to produce reorganized and reformatted data in an output array on the layer-2 chain.[21] The key characteristic of a rollup is that all data necessary to derive a given output array can be determined at any time by using only the data from the input array.[22] Rollups typically store both the input array

data and output array data on the layer-1 mainnet,[23] which acts as the "data availability layer" for the layer-2 protocol.[24]

By predominantly processing data off-chain and only relaying the underlying data and a summary of the computation results to the main chain, rollups drastically curtail gas expenses and amplify the database transaction processing rate.[25] Crucially, as data is embedded in blocks and consensus is attained on the layer-1 chain, rollups inherit the intrinsic security of the layer-1 chain.[26] Typically, layer 1, like Ethereum mainnet, is so widely used that there is widespread social consensus backing the protocol, which is why it is considered by most users to be virtually "immutable."[27]

Sequencers

Sequencers are the linchpins in most layer-2 rollup architectures, shouldering the responsibility of deciding the order of transactions to be put into blocks on the layer-2 chain.[28] What is colloquially called a "sequencer" is just one part of a larger rollup technology stack and is merely a combination of modular components of technology, which are generally under the control of a single person or entity.[29] Some of these components may overlap with other functions run by different, unaffiliated, uncoordinated third parties on the layer-2 network.[30] More specifically, a "sequencer" is a software-based mechanism used in layer-2 protocols to append inputs (*i.e.*, transaction data) to a rollup.[31]

In the same vein, "sequencing" simply refers to the process by which the sequencer performs a computation based only on a specific, pre-established algorithm (*i.e.*, code necessary to run a "rollup node"[32] and "execution engine"[33] based on a pre-agreed set of rules). This process is devoid of any discretion, other than the logic specified in the sequencer's software implementation. The sequencer accepts every input in the input array as it is submitted by the "batch submitter" (or, as it is sometimes called, the "proposer"). Then, the sequencer applies its programmatically enforced algorithm to the input array, the output from which the sequencer determines strictly based on protocol rules and is otherwise unable to alter in any way under normal circumstances.[34] This ensures that the sequencer is unable to submit a malicious batch of inputs that violates protocol rules.[35] The only possible reason a sequencer would not act objectively and based solely on its algorithm is if the system or code on which the sequencer is run is hijacked, rewritten, or corrupted, but many layer-2 protocols include additional software-based mechanisms to eliminate the risk.[36]

A sequencer, in effect, has no discretion whatsoever. Most layer-2 sequencers currently order transactions on a first-in-first-out basis, unless other prioritization options are transparently built in, and this is executed algorithmically, mirroring how validators include transactions on Ethereum.[37]

In particularly unlikely circumstances given other controls in place,[38] the worst-case scenario for a rogue sequencer cannot possibly amount to a theft of assets (*i.e.*, the sequencer inserting a transaction that moves an asset to an address controlled by a malicious actor rather than to an address controlled by the intended recipient). Instead, a more realistic concern is that a sequencer's operator could delay or sensor transactions[39] or propose an invalid "state root," causing the system to stall or to provide incorrect information to users.[40] To reduce or eliminate this risk, layer-2 protocols typically include multiple safeguards, such as waiting periods before withdrawals can be finalized and mechanisms for challenging and correcting invalid state roots.[41]

As a general matter, only the computer node running the sequencer is permissioned to write data to the rollup from the layer-2 chain.[42] This is with sole exception to the fact that, in many optimistic rollup systems,[43] users can bypass the sequencer and append inputs directly on the layer-1 network, which is essential for preserving censorship resistance,

albeit being slower and more costly.[44] Sequencers often perform two fundamental functions:[45] (1) interpreting data on the layer-1 chain to help determine the final order of layer-2 transactions; and (2) following protocol rules to provide an overall technical service accessible via remote procedure call ("RPC"),[46] which, on many protocols, allows users to submit database transactions and opt to pay a priority fee to obtain preferential ordering.

Solutions for scalability

While the ethos of blockchain gravitates toward "decentralization," the imperatives of scaling solutions can create some tension with this principle with the adoption of what are largely centralized sequencing mechanisms. As with the implementation of most technologies, trade-offs need to be considered: sequencers, when operated under the control of a single party, can offer speed and cost-efficiency, attributes that will likely be instrumental to expanding uses for, and promoting broader adoption of, blockchain technology.[47]

The main advantage of sequencers lies in their batch-processing capability. Only the "root" of these batches (*i.e.*, a smaller data set, derived from the full data set of all transactions) is relayed to the layer-1 blockchain, leading to a substantial reduction in on-chain data.[48] Yet, this methodology is not devoid of challenges. The "data availability problem" introduces a risk where off-chain data might become inaccessible, rendering the system's ability to revert to the main chain unfeasible.[49] Innovative solutions (like data sharding),[50] however, hold promise in alleviating this risk.[51]

Sequencers streamline data flow in the layer-2 ecosystem.[52] Users interface via RPC with sequencers, which subsequently process and sequence their transactions into blocks.[53] This data is then proposed, accepted, and incorporated into a block on the layer-1 chain.[54] The entire orchestration, spanning user interaction to block inclusion, is generally designed for maximum efficiency while also preserving many of blockchain's core virtues like transparency and security.

Mechanisms for accountability

"Proof systems" underpin trust in layer-2 solutions and form the bedrock of accountability for layer 2.[55] They ensure that layer-2 validators and other blockchains can trust the accuracy of the provided data.[56] Among the leading proofing solutions are "optimistic" and "zero-knowledge" rollups.[57] Zero-knowledge proof rollups, harnessing cutting-edge cryptographic techniques, offer swift transaction confirmations and enhanced privacy.[58] This does, however, come with the trade-off of increased rollup design complexity and diminished adaptability when it comes to the execution of code in the form of any "smart contract."[59] By contrast, optimistic rollups, which are more malleable in accommodating diverse smart contract logic, operate on a presumption of transaction validity.[60] This presumption introduces potential vulnerabilities, which layer-2 networks are able to mitigate using various challenge-response mechanisms.[61]

Sequencers, predominantly associated with optimistic rollups, play an indispensable role in layer-2 systems. The moniker "optimistic" stems from the default assumption of validity.[62] If a block (or the data record within it) is perceived as fraudulent or invalid, it can subsequently be challenged.[63] A valid challenge results in the reversion of the errors, with the challenger receiving a reward.[64] The sequencer system in optimistic rollups minimizes the number of transactions or data entries that can be relayed directly to the layer-1 mainnet, thereby dramatically improving its capacity to scale.[65] While zero-knowledge proof rollups do not intrinsically necessitate a sequencer in the same vein as optimistic rollups, a sequencer can theoretically be employed to sequence and batch transactions prior to generating the zero-knowledge proof for on-chain validation.[66] This can further refine the system's throughput and efficiency.[67]

As noted above, sequencers in optimistic rollups must be complemented with challenge-response mechanisms and other controls to ensure their accountability. The theoretical design of sequencers must be harmonized with practical oversight due to their pivotal role in transaction processing and sequencing.[68] The sequencer's central role introduces potential vulnerabilities, necessitating robust, tailored measures to mitigate risks.[69]

Importantly, while efficient, the sequencer's critical, often central role in layer-2 protocols introduces a potential single point of failure or manipulation.[70] Many layer-2 sequencer designs endeavor to implement controls that ensure credible neutrality, ensuring that no single entity can unduly influence the sequencer's operations.[71] Future projects might contemplate regular audits, transparent reporting, or community-driven checks and balances to ensure that sequencers function as intended.[72] In the absence of these kinds of measures, trust in optimistic layer-2 solutions could wane, given the sequencer's pivotal role.[73]

The role of verifiers

While sequencers play a pivotal role in processing and sequencing transaction data, "verifiers," participants who run "verifier nodes" on the layer-2 blockchain, typically serve as the guardians of data integrity in rollup solutions.[74] Often, there are many verifier nodes running on a layer-2 chain, computing largely the same code as the sequencer (*i.e.*, rollup node, execution engine, etc.).[75] This uniformity in code execution ensures consistency across the network. Depending on the specific layer-2 project, running a verifier node is typically permissionless, allowing for a distributed and trustless verification process.[76]

Verifiers are responsible for ensuring the correctness of all data submitted to the rollup.[77] They achieve this by verifying proofs and ascertaining the validity of state transitions on the layer-2 chain.[78] Unlike "validators,"[79] verifiers play only a passive role on layer 2, diligently checking the validity of data and replicating the outputs of the rollup computation.[80] This replication ensures that verifiers anticipate identical results as any other node operating solely based on the layer-1 blockchain's data.[81] For example, in scenarios where a "proposer"[82] – a layer-2 rollup mechanism responsible for proposing new data or transaction batches – introduces an error,[83] the verifier's node is typically equipped and incentivized to detect the discrepancy and raise an error by submitting a challenge.[84]

Layer-2 protocols are designed to prevent any identified errors from triggering on-chain repercussions. Some layer-2 projects, however, might one day explore the possibility of allowing a verifier node, or an entity running a node as a verifier, to submit a fault proof to rectify the error directly on-chain. Even in the current landscape, prevalent layer-2 protocols empower any layer-2 participant to run a node to verify the sequencer's accuracy in real time.[85]

Diverse deployment scenarios: A technical review

Blockchain technology's rapid progression has positioned layer-2 rollups as a promising solution to the scalability challenges of Ethereum and other blockchains.[86] As with any technological evolution, the journey toward widespread adoption is marked by a series of choices, each with its unique implications.

Developer choices

Layer-2 rollup technology, though nascent, provides layer-2 protocol developers with a range of options tailored to their specific requirements and goals.[87] These choices influence not just the technical architecture but also the security, scalability, and overall health of the ecosystem.[88] The processes and protocols governing how layer-2 rollup projects sequence and validate transactions can vary significantly[89] but, at least for optimistic rollups, broadly speaking, manifest in one of three different forms:

- *Centrally controlled sequencing*: Some developers opt for a centralized approach, where a single sequencing system and protocol processes data and orders transactions off-chain, sometimes even bypassing layer 2 altogether, and submit periodic summaries to the main (layer-1) blockchain.[90] While efficient, this model introduces potential vulnerabilities, including issues associated with a single, central point of failure.[91] Moreover, it may potentially be perceived as straying from the "decentralization" ethos foundational to blockchain.[92]
- *Shared sequencing*: Many rollup projects champion a shared sequencer approach, distributing the transaction ordering process across multiple nodes or validators on the layer-2 blockchain,[93] thereby reducing potential bottlenecks or central points of failure.[94] This method, often touted as a beacon of "decentralization," aims to prevent power centralization and ensure that every network participant has a voice.[95]
- *Hybrid approach*: Striving for equilibrium, some rollups combine elements of both centralized and community-driven operational mechanisms.[96] This approach varies widely in practice and effect, but generally seeks to harness the efficiency of centralization while retaining the trust and security synonymous with shared sequencing.[97]

The three broadly defined categories represent a scalable range. Notions of "centralization" and "decentralization" are helpful in concept but fluid, broad, and ill-defined in meaning. While software components that do not live on a public blockchain are all inherently "centralized" in some way, generally, various sequencer elements can often be distributed, decoupled from a single provider and run separately by different, unaffiliated, uncoordinated parties.[98] For example, some sequencers might run both the batch submitter protocol (*i.e.*, submitting inputs to layer 1) and the output proposal submitter protocol (*i.e.*, submitting outputs to layer 1), even though these are entirely independent software programs.[99] The output proposal process for most layer-2 projects could potentially be made permissionless, further limiting the adverse impact of an incapable or misbehaving sequencer.[100]

Importantly, decentralization is a spectrum, not an absolute state. Even today's "centralized" sequencers are not as centrally controlled as they may be perceived. Accountability systems and checks can provide assurances of a robust and transparent system. These might include mechanisms for providing real-time public visibility into the system's integrity, allowing anyone to bypass the sequencer and transact directly on the rollup on layer 1, and controlling potential vulnerabilities, like with the use of challengers, proposers, guardians, and upgrade keys.[101]

Scalability *vs* security

The primary appeal of layer-2 rollups is scalability.[102] Scalability and security are intricately linked; however, enhancing one without due consideration to the other can introduce material vulnerabilities. Developers must tread this delicate balance to ensure that, as transaction speeds increase, the system's integrity remains uncompromised.

For example, shared sequencers can offer enhanced transparency but also might introduce new challenges, like ensuring consistent data availability across the layer-2 network.[103] In a shared sequencing system, data must be readily accessible across various nodes or validators.[104] If any part of the data becomes unavailable or is delayed in its dissemination, it can cause system outages, leading to delays or failures.[105] To counteract these risks, optimistic rollups often mandate sequencers to post full transaction data when publishing to the layer-1 blockchain, ensuring continuity even if a sequencer goes offline.[106] This helps to ensure that, even if a sequencer goes offline, the sequencer (or another sequencer) can use the transaction data to reconstruct the state of the rollup and continue producing blocks on layer 2.[107]

User experience implications

The design and deployment choices of layer-2 solutions invariably affect the end user.[108] On the one hand, a solution that prioritizes rapid transaction confirmations might be well suited for platforms requiring real-time interactions.[109] On the other hand, a solution that emphasizes data availability and consistency might better cater to applications with high data retrieval demands.[110] The sequencing of transactions, whether centrally managed or in some way distributed, can also influence transaction costs, confirmation times, and overall user trust in the system.[111]

In a rollup protocol where transaction sequencing is controlled by a single entity or a select group, efficiencies in ordering and processing can allow reduced transaction fees.[112] Alternatively, this entity could also theoretically exploit its position to impose higher fees, especially if users have limited alternatives.[113] By contrast, depending on the incentive structures in place, a shared sequencing approach can potentially drive fees to more competitive rates where multiple nodes or validators participate in the ordering process.[114]

More centrally controlled sequencing systems might also offer faster confirmation times due to streamlined processing.[115] Shared sequencing systems, however, while benefiting from redundancy, might face longer confirmation times due to the need for consensus.

Choices made by layer-2 project teams can also have profound implications on user trust. In layer-2 networks with a centrally operated sequencer, trust hinges on the reputation and reliability of the operator. If the operator maintains a record of transparency, security, and fairness, users may be more likely to place significant confidence in the system.[116] Any missteps, however, such as perceived censorship or unfair fee structures, have the potential to erode that confidence much more rapidly than it was amassed.[117] Contrarily, shared sequencing systems distribute trust across multiple participants, potentially allowing users to feel more secure knowing that no single person or group has undue control over transaction ordering.[118]

The developer's playbook: Merging tech with legal prudence

The fusion of technology and law, especially in the realm of blockchain, requires a careful and intelligent approach. As layer-2 solutions continue to evolve, developers must be both innovative and sensitive to a range of potential legal issues.

Overall, layer-2 rollup protocols require more than impeccable code; they must also embrace a broad spectrum of best practices. Rigorous testing is required to ensure that the system can handle real-world scenarios, and continuous monitoring should be used to detect and address potential vulnerabilities.[119] Moreover, by staying abreast of the latest research in blockchain, developers can integrate cutting-edge solutions, enhancing both efficiency and security. A hallmark of successful deployments is transparency, and this is no less true in sequencer operations.[120] By being open about their processes, developers can foster community trust and potentially mitigate any regulatory concerns that may arise.

Legal collaboration

Navigating the intricacies of layer-2 sequencing requires a keen understanding of both its technical and potential legal facets. The design choices, from sequencer control mechanisms to operational transparency, can have far-reaching legal implications. While sequencers play a pivotal role in the layer-2 ecosystem, they are only one part of a broader tableau. Developers seeking to establish a new layer-2 network must be cognizant of this bigger picture, recognizing that, depending on the choices they make, their project may potentially

come under regulatory scrutiny. Importantly, the global legal landscape is dynamic and often not easily predictable: what might not be cause for legal concern to layer-2 developers today could very well be contentious tomorrow, however misplaced that future legal or regulatory anxiety might be.

While the underlying code of a layer-2 solution might be technically sound, its practical, real-world effects could potentially invite legal scrutiny. The level of influence and control a developer or any other entity wields over specific functions within the rollup can potentially be a focal point for regulators seeking to target blockchain-based projects and infrastructure. For instance, a rollup project that disproportionately influences transaction sequencing or inadvertently centralizes control over critical functions (like sequencing) without building in proper guardrails might attract regulatory attention, even if unintentional. If a single, definable entity has the power to dictate the order of transactions or blocks, validate data, or influence fees, then that entity could possibly be perceived as having some improper level of "control" and potentially triggering scrutiny.

Engaging with legal experts early in the development phase is not just a precautionary measure, but a strategic imperative. Collaboration can illuminate potential pitfalls, allowing layer-2 project developers to make informed decisions that align with both their technological ambitions and the ever-evolving legal landscape. By understanding the potential legal ramifications of their design choices, developers can craft solutions that are not only innovative but also compliant with current and readily foreseeable regulatory frameworks.

"Future proofing" deployments

In the ever-developing world of blockchain, adaptability can be a key to success. Layer-2 solutions must be designed with an eye toward the future, capable of accommodating both technological innovations and potential shifts in regulatory paradigms across various jurisdictions. This might involve adopting modular design principles, championing open-source development, or conducting regular audits. By taking distributed ledger technology's evolutionary trajectory into consideration early in the development of any layer-2 protocol, developers can better ensure their solutions remain relevant and robust and do not run afoul of potentially applicable restrictions.

One of the best ways to stay on top of developments is to stay engaged with the blockchain community, which is not just a user base, but a collaborative ecosystem composed of a community of individuals with a broad range of valuable insights and expertise. By actively seeking feedback, developers can refine their layer-2 solutions, helping to ensure that they meet the community's needs and expectations while remaining cognizant of relevant developments in law, regulation, and best practices. This iterative approach is not only likely to enhance project efficacy but also to engender trust and foster a sense of shared purpose and vision.

Looking ahead: The future of layer-2 tech

The blockchain ecosystem is in a constant state of growth and transformation, with layer-2 rollup technology currently at the forefront, paving the way for novel applications and use cases.[121] As the demand for scalable and efficient blockchain solutions grows, so too does the drive for innovation in layer-2 rollup technology.

Prospective developments

One of the primary objectives of layer-2 rollups is to address the scalability challenges inherent in many blockchain networks.[122] Therefore, the most recent advancements have

largely been focused on optimizing transaction throughput without compromising on security. This means that future layer-2 solutions might be able to safely handle a significantly higher number of transactions per second than current systems. With the growing concerns around data privacy and security, developers are also likely to push toward integrating advanced cryptographic techniques into layer-2 rollups. These techniques would likely not only ensure transaction privacy but also play a crucial role in enhancing the overall security of the system.

As the blockchain space becomes more fragmented with various chains serving different purposes, the need for these chains to communicate with each other becomes paramount. Future innovations in layer-2 rollups will likely focus on ensuring seamless interoperability between different blockchains, allowing for a more integrated and cohesive blockchain ecosystem.[123] As these technologies mature and are used to connect otherwise separate, siloed networks – laying the foundation for a more robust and cohesive web3 – the potential applications and use cases for layer-2 rollups, and for blockchain more broadly, are theoretically infinite.

Key takeaways

Layer-2 rollups, while transformative, are but one component in the vast and diverse machinery of maturing blockchain technologies. Before jumping to any conclusions about how these technologies are being deployed, lawyers and policymakers would be wise to exercise restraint and take the time to understand granularly how each involved mechanism functions. As with any technology, the practical implications and real-world effects are what truly matter. Critically, like with any software component used by participants and intermediaries in traditional data networks and payments systems, sequencers and every other software component of layer-2 rollups are designed to be impartial, with no discretion to exclude data or transactions that they were not specifically programmed to include.[124]

The complexities of layer-2 sequencing technology underscore the importance of attorneys and regulators assuming a nuanced understanding and approach. Laws and regulations need not prescribe any requirements or limitations on blockchain development or any specific technological functions like sequencing. Likely no public policy that applies broadly to blockchain developers or participants would be adequately flexible and permissive, let alone necessary or appropriate. For instance, a layer-2 sequencer, while pivotal, is only one component of rollup systems and the evolving blockchain landscape. Rigidly prescribed rules or responsibility would likely only hinder a jurisdiction's technological advances and set back the security, economy, and welfare of its people in an increasingly competitive global stage. Meanwhile, most regulators and enforcement authorities have existing frameworks to apply if a person or group's activity raises concerns of willful fraud or consumer harm, without boxing every entity into a specifically financial regulatory framework.

The providers of data infrastructure, as a matter of best practices (and often compelled by independently applicable regulatory requirements),[125] must do their own due diligence before using any third-party software or participating in any network. The third-party software and infrastructure providers used by traditional intermediaries, however, are not – and need not be – subject to any direct regulatory requirements.[126] Therefore, similarly, it would be reasonable to conclude that those building out elements of web3 infrastructure should not be directly regulated as financial intermediaries just because their infrastructure might be indirectly utilized in financial transactions and should generally not bear responsibility for network participants, software users, or their applications of what is, in a controlled environment, completely neutral technology.[127]

Call to action

The future state of blockchain and the potential advancements it holds hinge on collaboration. Developers, users, legal experts, and policymakers must all engage in ongoing dialogue to foster innovation while ensuring a safe and resilient web3 ecosystem. By bridging the gap between technical innovation and legal prudence, we can pave the way for a future where technology and law coexist in synergy, driving progress while continuing to uphold principles of network neutrality, fairness, verifiable reliability, and security.

* * *

Endnotes

1. Notably, a "database transaction" is a technical term that does not necessarily have any financial implications. A database transaction is a unit of work in a database management system, treated consistently and reliably, separate from other transactions. It typically signifies a database modification. *See* Antonello Zanini, *Database Transactions 101: The Essential Guide*, Db Visualizer: theTable (Feb. 14, 2023), https://www.dbvis.com/thetable/database-transactions-101-the-essential-guide ; Carlos Garcia, *What is a Database Transaction?*, AppMaster: Blog (Jan. 18, 2023); *What is a Transaction?*, Microsoft Windows App Development: Documentation (Jan. 7, 2021), https://learn.microsoft.com/en-us/windows/win32/ktm/what-is-a-transaction?redirectedfrom=MSDN
2. *See* George Konstantopoulos, *Almost Everything You Need to Know About Optimistic Rollups*, Paradigm (Jan. 28, 2021), https://www.paradigm.xyz/2021/01/almost-everything-you-need-to-know-about-optimistic-rollup ; *Layer 2: Ethereum for Everyone*, Ethereum, https://ethereum.org/en/layer-2 (last visited Aug. 24, 2023) (providing more detailed descriptions of layer-2 rollup networks, how they function, and how they interact with their related layer-1 network).
3. *See* Vitalik Buterin, *Proposed Milestones for Rollups Taking Off Training Wheels*, Ethereum Magicians Forum (Nov. 3, 2022), https://ethereum-magicians.org/t/proposed-milestones-for-rollups-taking-off-training-wheels/11571; Kyle Charbonnet, *An Introduction to Optimism's Optimistic Rollup*, Medium: Privacy & Scaling Explorations (Jul. 1, 2021), https://medium.com/privacy-scaling-explorations/an-introduction-to-optimisms-optimistic-rollup-8450f22629e8; *How Do Optimistic Rollups Work: The Complete Guide*, Alchemy: Overviews: Optimistic Rollups (rev. Mar. 14, 2023), https://www.alchemy.com/overviews/optimistic-rollups
4. *See The Espresso Sequencer*, Espresso Systems (HackMD) (rev. Mar. 20, 2023), https://hackmd.io/@EspressoSystems/EspressoSequencer; *Layer-2 Scaling Solutions*, Pontem Network: Pontem Blog, https://pontem.network/posts/layer-2-scaling-solutions-2 (last visited Aug. 24, 2023).
5. *See The Sequencer and Censorship Resistance*, Arbitrum Docs: Sequencer (rev. Aug. 18, 2023), https://developer.arbitrum.io/sequencer
6. Like with other technologies, the degree of control exerted by sequencers, the transparency (or lack thereof) of their operations, and the choices made in their deployment could potentially draw scrutiny from regulators. It is worth noting that the legal landscape surrounding layer-2 sequencers remains largely uncharted; no sequencer deployment scenario has been rigorously tested or challenged under potentially applicable laws or regulations. *See generally* Angela Angelovska-Wilson *et al.*, *Decentralized Finance: The Revolution Continues, Current*

Regulations and Impacts of Cross-chain Bridge Solutions, Global Legal Insights, Blockchain & Cryptocurrency Laws and Regulations 2023 (Oct. 2022), https://www.globallegalinsights.com/practice-areas/blockchain-laws-and-regulations/05-decentralized-finance-the-revolution-continues-current-regulations-and-impacts-of-cross-chain-bridge-solutions

7. *See Espresso Sequencer Architecture: System Overview*, Espresso Docs, *supra* note 6; *Sequencers*, Metis Docs: Protocol in Detail (rev. Aug. 4, 2022), https://docs.metis.io/dev/the-architecture-of-the-metis-smart-l2/sequencers; *The Sequencer and Censorship Resistance*, Arbitrum Docs, *supra* note 5.
8. *See id*.
9. For the purposes of this chapter, we presuppose that sequencers are programmed to follow an objective protocol as they largely are in the layer-2 iterations discussed by this chapter. Notably, however, as with most software, sequencing software can be programmed differently depending on the functions it is designed to perform, including where a sequencer may be built with a different set of transaction ordering policies and priorities in mind.
10. *See infra* "Sequencers".
11. *See* Shannon Wu, *Bridging the Gap Between Traditional and Decentralized Finance*, Forbes (Aug. 31, 2020), https://www.forbes.com/sites/forbestechcouncil/2020/08/31/bridging-the-gap-between-traditional-and-decentralized-finance; Angela Angelovska-Wilson *et al.*, *supra* note 7.
12. *See* Shannon Wu, *supra* note 13; Primavera De Filippi *et al.*, *The Alegality of Blockchain Technology*, Oxford Academic: Policy & Society (Feb. 16, 2022), https://academic.oup.com/policyandsociety/article/41/3/358/6529327
13. *See* Jason Cohen, *4 Companies Control 67% of the World's Cloud Infrastructure*, PC Magazine: News: The Why Axis (Dec. 29, 2021), https://www.pcmag.com/news/four-companies-control-67-of-the-worlds-cloud-infrastructure; Felix Richter, *Amazon Maintains Lead in the Cloud Market*, Statista (Aug. 8, 2023), https://www.statista.com/chart/18819/worldwide-market-share-of-leading-cloud-infrastructure-service-providers
14. *See* Clare Stouffer, *23 Cloud Security Risks, Threats, and Best Practices to Follow*, Norton: Blog (Jul. 11, 2023), https://us.norton.com/blog/privacy/cloud-security-risks
15. *See generally* Primavera De Filippi *et al.*, *supra* note 14.
16. *See Scaling Overview*, Ethereum Docs: Scaling (rev. Apr. 7, 2023), https://ethereum.org/en/developers/docs/scaling
17. "Gas" are the transaction fees paid by network users, primarily to transaction validators.
18. *See Layer-2 Scaling Solutions*, Pontem Network, *supra* note 3; *Optimistic Rollups*, Ethereum Docs: Scaling (rev. Jun. 28, 2023), https://ethereum.org/en/developers/docs/scaling/optimistic-rollups
19. *See Scaling Overview*, Ethereum Docs, *supra* note 18; *Shared Sequencing: Defragmenting the L2 Rollup Ecosystem*, Espresso Systems (HackMD) (rev. May 2, 2023), https://hackmd.io/@EspressoSystems/SharedSequencing
20. *See How Do Optimistic Rollups Work: The Complete Guide*, Alchemy, *supra* note 2.
21. In simpler terms, consider the equation 2+2=4 as an example. Here, the input array consists of the numbers 2 and 2, and the output array is 4. The function, in this case, is basic arithmetic (*i.e.*, addition).

22. *See Optimistic Rollups*, Ethereum Docs, *supra* note 20 (discussing how all data necessary to reconstruct the rollup's state is stored on-chain, ensuring that, even if the sequencer disappears, users can still retrieve their funds); *see*, *e.g.*, Kyle Charbonnet, *supra* note 2 (highlighting the Optimism layer-2 protocol's use of a modified version of the Ethereum Virtual Machine, or "EVM," to ensure that layer-2 transactions are "replayable" on both layer-1 and layer-2 chains with consistent outcomes).
23. The process can be illustrated, in reduced form, by three steps or three states: input array (layer 1) > function (rollup node software) > output array (layer 2).
24. *See Optimistic Rollups*, Ethereum Docs, *supra* note 20.
25. *See id*.
26. In effect, the only way someone could change the established, historical state of the layer-2 blockchain is by changing the state of the Ethereum smart contract itself. This is only possible if the person can break Ethereum, a network renowned for decentralization and security. *See id*.
27. *See*, *e.g.*, *Espresso Sequencer Architecture: System Overview*, Espresso Docs , *supra* note 6 (emphasizing that the sequencer's consistent communication with the layer-1 chain is designed to ensure trustless state checkpoints); *OP Mainnet's Security Model*, Optimism Community Docs (rev. Aug. 23, 2023), https://community.optimism.io/docs/security-model (discussing how Optimism layer-2 blocks are stored on the Ethereum blockchain using a non-contract address to minimize layer-1 gas costs) (also discussing how, once submitted as call data on Ethereum, these blocks are immutable once included in a sufficiently attested layer-1 block).
28. *See Optimistic Rollups*, Ethereum Docs, *supra* note 20.
29. *See* Darren Kleine, *supra* note 16; *Overview: The Lifecycle of an Arbitrum Transaction*, Arbitrum Docs: Tx Lifecycle (rev. Aug. 18, 2023), https://developer.arbitrum.io/tx-lifecycle
30. *See Overview: The Lifecycle of an Arbitrum Transaction*, Arbitrum Docs, *supra* note 31; *Shared Sequencing: Defragmenting the L2 Rollup Ecosystem*, Espresso Systems (HackMD), *supra* note 21.
31. *See Scaling Overview*, Ethereum Docs: Scaling (rev. Apt. 7, 2023), https://ethereum.org/en/developers/docs/layer-2-scaling
32. A "rollup node" is a specialized node that the sequencer runs on the mainnet to submit batch transaction data.
33. The "execution engine" is the component of the sequencer's code that allows the sequencer to execute and process incoming transactions based on pre-agreed ordering rules.
34. *See Designing the Espresso Sequencer: Combining HotShot Consensus with Tiramisu DA*, Espresso Systems (HackMD) (rev. Jul. 20, 2023), https://hackmd.io/@EspressoSystems/HotShot-and-Tiramisu; *see generally* Eric Rykwalder, *The Math Behind the Bitcoin Protocol*, CoinDesk (Oct. 19, 2014), https://www.coindesk.com/markets/2014/10/19/the-math-behind-the-bitcoin-protocol
35. *See The Sequencer and Censorship Resistance*, Arbitrum Docs, *supra* note 5; *Rollup Sequencers are Centralized: And That's Fine*, Blockworks, *supra* note 16.
36. *See infra* "Mechanisms for accountability" and "Developer choices". Markedly, since various protocols could implement different ordering policies (*e.g.*, first-come-first-serve, time enhancing, MEV maximizing), with differing use cases, aims, and risks, this may not always be true of all protocols. *See also supra* note 13.

37. *See* Vitalik Buterin, *What Would a Rollup-Centric Ethereum Roadmap Look Like?*, Ethereum Magicians Forum (Oct. 2, 2020), https://ethereum-magicians.org/t/a-rollup-centric-ethereum-roadmap/4698; *Overview: The Lifecycle of an Arbitrum Transaction*, Arbitrum Docs, *supra* note 31; *Optimistic Rollups*, Ethereum Docs, *supra* note 20.
38. *See infra* "Mechanisms for accountability" and "Developer choices".
39. These are some of the primary considerations compelling the use of decentralized sequencers. *See infra* "Developer choices".
40. *See The Sequencer and Censorship Resistance*, Arbitrum Docs, *supra* note 5; *Optimistic Rollups*, Ethereum Docs, *supra* note 20.
41. *See Optimistic Rollups*, Ethereum Docs, *supra* note 20; *L2 Output Root Proposals Specification*, Github: Optimism: Specs (rev. Jun. 26, 2023), https://github.com/ethereum-optimism/optimism/blob/develop/specs/proposals.md
42. *See Rollup Sequencers are Centralized: And That's Fine*, Blockworks, *supra* note 16.
43. Optimistic rollups are systems that operate on a presumption of transaction validity for all batch data submitted by the sequencer to the layer-1 chain. *See infra* "Mechanisms for accountability".
44. *See Optimistic Rollups*, Ethereum Docs: Scaling, *supra* note 20; *see generally infra* note 85 (discussing layer-2 rollup state challenge processes).
45. *See The Sequencer and Censorship Resistance*, Arbitrum Docs: Sequencer, *supra* note 5; *Espresso Sequencer Architecture: System Overview*, Espresso Docs, *supra* note 6.
46. A remote procedure call (or "RPC") is a broader blockchain-related concept referring to the method by which users or applications communicate with a blockchain node. When working with layer-2 solutions like rollups, RPC endpoints can be crucial. They allow users and applications to send transactions, query balances, fetch data, and more, specifically for that layer-2 environment. As rollups and other layer-2 solutions have their own state and data separate from the main Ethereum chain, they often provide their own RPC endpoints for direct interaction. *See Scaling Overview*, Ethereum Docs, *supra* note 33; *see generally What Is an RPC Node: A Comprehensive Guide*, Blockchain Council: Understanding Blockchain, https://www.blockchain-council.org/blockchain/what-is-an-rpc-node (last visited Aug. 24, 2023) (providing a detailed overview of RPCs).
47. *See Rollup Sequencers are Centralized: And That's Fine*, Blockworks, *supra* note 16; *Optimistic Rollups*, Ethereum Docs, *supra* note 20.
48. *See Optimistic Rollups*, Ethereum Docs, *supra* note 20.
49. *See* Kyle Charbonnet, *supra* note 2; *Optimistic Rollups*, Ethereum Docs, *supra* note 20.
50. Sharding is a scaling solution for blockchains that increases the number of transactions a blockchain can process by splitting the network into smaller pieces, called shards. Each shard processes its own micro-blocks. Sharding can help address the data availability problem by ensuring that even if one shard becomes unavailable, the others remain operational. *See Sharding FAQ*, Github: Ethereum: Wiki (rev. May 24, 2022), https://github.com/ethereum/wiki/wiki/Sharding-FAQ
51. *See id*.; *Ethereum 2.0 FAQ*, Consensys: Knowledge Base, https://consensys.net/knowledge-base/ethereum-2/faq (last visited Aug. 24, 2023).
52. *See The Espresso Sequencer*, Espresso Systems (HackMD), *supra* note 3; *The Sequencer and Censorship Resistance*, Arbitrum Docs, *supra* note 5; *Espresso Sequencer Architecture: System Overview*, Espresso Docs, *supra* note 6.
53. *See Overview: The Lifecycle of an Arbitrum Transaction*, Arbitrum Docs, *supra* note 31; *see also The Sequencer and Censorship Resistance*, Arbitrum Docs, *supra* note 5 (discussing how the Arbitrum sequencer receives transactions directly from a client or via layer 1 through a "delayed inbox").

54. *See The Sequencer and Censorship Resistance*, Arbitrum Docs, *supra* note 5.
55. *See Introduction to zkSync for Developers*, zkSync Docs (rev. Feb. 16, 2023), https://zksync.io/dev/tutorial.html; *Optimistic Rollups*, Ethereum Docs, *supra* note 20.
56. *See Introduction to Optimism*, Optimism (Github): Specs (rev. Apr. 6, 2023), https://github.com/ethereum-optimism/optimism/blob/develop/specs/introduction.md; Alex Gluchowski, *Optimistic vs. ZK Rollup: Deep Dive*, Medium: Matter Labs Blog (Nov. 4, 2019), https://blog.matter-labs.io/optimistic-vs-zk-rollup-deep-dive-ea141e71e075; *Rollups*, Paradigm Research, https://research.paradigm.xyz/rollups (last visited Jul. 22, 2023); *What's the Difference Between Arbitrum Rollup and Arbitrum AnyTrust?*, Arbitrum Docs: FAQs: Protocol (rev. Aug. 18, 2023), https://developer.arbitrum.io/faqs/protocol-faqs; *see also Optimistic Rollups*, Ethereum Docs, *supra* note 20 (emphasizing that security of optimistic rollups is based on the main Ethereum chain, thus ensuring trust in the provided data).
57. *See* Alex Gluchowski, *supra* note 57.
58. *See Introduction to Optimism*, Optimism (Github), *supra* note 57.
59. *See* Alex Gluchowski, *supra* note 57.
60. *See id*.; *Introduction to Optimism*, Optimism (Github), *supra* note 57; *see also Optimistic Rollups*, Ethereum Docs, *supra* note 20 (explaining that, because optimistic rollup protocols largely execute transactions off-chain, they must assume that all transactions are valid without proving transaction validity); *Layer-2 Scaling Solutions*, Pontem Network, *supra* note 3 (emphasizing that optimistic rollups assume that all transactions are valid without proving transaction validity).
61. *See Optimistic Rollups*, Ethereum Docs, *supra* note 20; *Introduction to Optimism*, Optimism (Github): Specs, *supra* note 57.
62. *See Scaling Overview*, Ethereum Docs, *supra* note 18.
63. *See How Do Optimistic Rollups Work: The Complete Guide*, Alchemy, *supra* note 2; *Optimistic Rollups*, Ethereum Docs, *supra* note 20; Alex Gluchowski, *supra* note 57.
64. *See How Do Optimistic Rollups Work: The Complete Guide*, Alchemy, *supra* note 2; Alex Gluchowski, *supra* note 57.
65. *See Scaling Overview*, Ethereum Docs, *supra* note 18.
66. *See id*.
67. *See id*.; *How Do Optimistic Rollups Work: The Complete Guide*, Alchemy, *supra* note 2; Alex Gluchowski, *supra* note 57.
68. *See The Espresso Sequencer*, Espresso Systems (HackMD), *supra* note 3; *Rollup Sequencers are Centralized: And That's Fine*, Blockworks, *supra* note 16.
69. *See The Espresso Sequencer*, Espresso Systems (HackMD), *supra* note 3.
70. This is often the case except with sequencers with some level of decentralization. *See infra* "Developer choices"; *see*, *e.g.*, *Shared Sequencing: Defragmenting the L2 Rollup Ecosystem*, Espresso Systems (HackMD), *supra* note 21.
71. *See*, *e.g.*, *The Espresso Sequencer*, Espresso Systems (HackMD), *supra* note 3 (demonstrating how neutrality promotes accountability and allows for enhanced interoperability so that transactions can be processed in a manner that is consistent across various rollups).
72. *See Rollup Sequencers are Centralized: And That's Fine*, Blockworks, *supra* note 16.
73. *See id*.
74. *See Scaling Overview*, Ethereum Docs, *supra* note 33.
75. *See id*.
76. *See* George Konstantopoulos, *supra* note 1; *Optimistic Rollups*, Ethereum Docs, *supra* note 20; *What's the Difference Between Arbitrum Rollup and Arbitrum AnyTrust?*, Arbitrum Docs, *supra* note 57.

77. *See generally Introduction to Optimism*, Optimism (Github), *supra* note 57.
78. *See id*.
79. "Verifiers" should not be confused with "validators" on a blockchain network. Verifiers do not produce blocks or participate in consensus like validators on a blockchain; instead, they only passively check the validity of data. *See 2023 Metis L2 Roadmap*, Metis Knowledge Base (rev. Apr. 5, 2023), https://metis.io/knowledge/2023-metis-l2-roadmap; Metis Andromeda (2beat): Scaling, https://l2beat.com/scaling/projects/metis (last visited Aug. 24, 2023); *What's the Difference Between Arbitrum Rollup and Arbitrum AnyTrust?*, Arbitrum Docs, *supra* note 57.
80. *See What's the Difference Between Arbitrum Rollup and Arbitrum AnyTrust?*, Arbitrum Docs, *supra* note 57; *Introduction to Optimism*, Optimism (Github), *supra* note 57.
81. *See id*.
82. While sequencers often assume the same role as a "proposer" in many layer-2 systems, this association is not mandatory. For example, sequencers should not assume this role in systems that allow permissionless output proposals, because the role of a "proposer" mechanism in this instance becomes entirely unauthenticated.
83. For instance, based on the simplified example in arithmetic from "Technical foundations of layer-2 sequencing", an error might be providing "5" as the output for the inputs of "2+2." *See supra* note 23.
84. The verifier typically must submit any challenge as a transaction to the same smart contract on the mainnet. A successful challenge requires the verifier to specify the particular transaction or state transition that the verifier believes is invalid. In some cases, if there is a dispute that cannot be resolved on the rollup, the layer-2 protocol might have a mechanism to "fall back" to layer 1 for resolution, though typically more costly and time-consuming. This typically involves executing the challenged transaction on the mainnet to determine its validity. *See Scaling Overview*, Ethereum Docs, *supra* note 18.
85. Participants can then take corrective actions, such as exiting the system through a direct layer-1 transaction or signaling to the broader community about potential issues with the sequencer's operator. *See* Alex Gluchowski, *supra* note 57.
86. *See generally* Primavera De Filippi *et al.*, *supra* note 14.
87. *See generally id*.; *Layer 2 Scaling*, Ethereum Docs: Scaling (rev. Apr. 7, 2023), https://ethereum.org/en/developers/docs/layer-2-scaling/#rollups; *Scaling Overview*, Ethereum Docs, *supra* note 18; *see*, *e.g.*, *Shared Sequencing: Defragmenting the L2 Rollup Ecosystem*, Espresso Systems (HackMD), *supra* note 21 (highlighting choices available to developers between optimistic and zero-proof rollups); *The Sequencer and Censorship Resistance*, Arbitrum Docs, *supra* note 5 (discussing an array of options in setting up sequencer operations).
88. *See How Do Optimistic Rollups Work: The Complete Guide*, Alchemy, *supra* note 2; *Rollup Sequencers are Centralized: And That's Fine*, Blockworks, *supra* note 16.
89. *See id*.; *The Sequencer and Censorship Resistance*, Arbitrum Docs, *supra* note 5 (showcasing the variability in processes for sequencing and validating transactions).
90. *See generally Scaling Overview*, Ethereum Docs, *supra* note 18; *see*, *e.g.*, *The Sequencer and Censorship Resistance*, Arbitrum Docs, *supra* note 5 (detailing use of fully centrally controlled sequencer operations but contemplating more decentralized mechanisms for future iterations of the protocol, such as by involving a distributed committee of sequencers).

91. *See Shared Sequencing: Defragmenting the L2 Rollup Ecosystem*, Espresso Systems (HackMD), *supra* note 21 (emphasizing the risks of having a single sequencer, which can become a single point of failure, leading to potential censorship and monopolistic behaviors); *see generally supra* "Mechanisms for accountability".
92. *See* Kyle Charbonnet, *supra* note 2 (acknowledging that relying on a single sequencer represents the departure from the aims of a fully decentralized model); *Introduction to Boba Network for Developers*, Boba Docs: For Developers, https://docs.boba.network/for-developers/developer-start (last visited Aug. 24, 2023) (underscoring how reliance on a sequencer could be seen as a move away from full decentralization); *see also Espresso Sequencer Architecture: System Overview*, Espresso Docs, *supra* note 6 (emphasizing the importance of credible neutrality and alignment with Ethereum's ethos).
93. *See*, *e.g.*, *Shared Sequencing: Defragmenting the L2 Rollup Ecosystem*, Espresso Systems (HackMD), *supra* note 21 (suggesting that a shared sequencer can connect liquidity and applications between rollups, enhancing user experience, and increasing the utility of individual rollups).
94. *See id*.
95. *See* Radius (radius.xyz), *Shared Sequencer for MEV Protection and Profitable Marketplace*, EthResearch (Apr. 16, 2023), https://ethresear.ch/t/shared-sequencer-for-mev-protection-and-profitable-marketplace/15313; *Rollup Sequencers are Centralized: And That's Fine*, Blockworks, *supra* note 16.
96. *See*, *e.g.*, *Introduction to Boba Network for Developers*, Boba Docs: For Developers, *supra* note 93 (suggesting use of distributed checking mechanisms in combination with a centrally operated sequencer); Roderic Puah, *Metis Andromeda: The Latest Layer 2 Protocol on Ethereum*, Switcheo Research: Blog (Mar. 8, 2022), https://blog.switcheo.com/metis-andromeda (detailing use of multiple sequencers pooled into on-chain units called "decentralized autonomous companies").
97. *See* Peter Mell *et al.*, *Blockchain Technology Overview*, Dep't of Com., Nat. Inst. of Standards & Tech., NISTIR 8202 (Oct. 2018), https://nvlpubs.nist.gov/nistpubs/ir/2018/NIST.IR.8202.pdf; *How Do Optimistic Rollups Work: The Complete Guide*, Alchemy, *supra* note 2.
98. *See*, *e.g.*, *Espresso Sequencer Architecture: System Overview*, Espresso Docs, *supra* note 6.
99. *See*, *e.g.*, *Batch Submitter*, Optimism (Github): Specs (rev. Jan. 13, 2023), https://github.com/ethereum-optimism/optimism/blob/develop/specs/batcher.md; *L2 Output Root Proposals Specification*, Github: Optimism: Specs, *supra* note 32.
100. *See L2 Output Root Proposals Specification*, Github: Optimism: Specs, *supra* note 32; Vitalik Buterin, *supra* note 39.
101. *See An Incomplete Guide to Rollups*, Vitalik.ca (Jan. 5, 2021), https://vitalik.ca/general/2021/01/05/rollup.html
102. *See Scaling Overview*, Ethereum Docs, *supra* note 33.
103. *See Layer 2 Scaling*, Ethereum Docs: Scaling, *supra* note 88.
104. *See Espresso Sequencer Architecture: System Overview*, Espresso Docs, *supra* note 6 (illustrating the flow of information throughout the system, starting from clients, passing through the sequencer, moving to integrated rollups, and culminating in certification and checkpointing on layer 1); *see generally Shared Sequencing: Defragmenting the L2 Rollup Ecosystem*, Espresso Systems (HackMD), *supra* note 21 (touting the sequencer as a tool for defragmenting the layer-2 landscape and connecting liquidity, applications, and shared data among different rollups).

105. *See* George Konstantopoulos, *supra* note 1. Regardless of whether sequencing operations are centrally controlled or dispersed, there may always be a potential risk, however small, of a sequencer going rogue or even offline. *See Shared Sequencing: Defragmenting the L2 Rollup Ecosystem*, Espresso Systems (HackMD), *supra* note 21; *see*, *e.g.*, Sage Young, *Arbitrum Temporarily Stopped Processing Due to Software Bug*, CoinDesk: Technology (Jun. 7, 2023), https://www.coindesk.com/tech/2023/06/07/arbitrum-temporarily-stopped-processing-due-to-software-bug (reporting how the Arbitrum layer 2 went out of service for several hours due to a bug in the sequencer and a resulting transaction backlog that stressed the network).
106. *See Optimistic Rollups*, Ethereum Docs, *supra* note 20. While shared sequencers can reduce central points of failure and enhance transparency, they often require implementing additional mechanisms to ensure that data is consistently available and can be efficiently retrieved by all network participants. *See Shared Sequencing: Defragmenting the L2 Rollup Ecosystem*, Espresso Systems (HackMD), *supra* note 21.
107. *See* Kyle Charbonnet, *supra* note 2; *The Sequencer and Censorship Resistance*, Arbitrum Docs, *supra* note 5.
108. *See Optimistic Rollups*, Ethereum Docs, *supra* note 20 (highlighting the impact of various layer-2 features on the end user, such as the need for users to be online to challenge fraudulent transactions and any delays in withdrawals); *see*, *e.g.*, *Layer-2 Scaling Solutions*, Pontem Network, *supra* note 3 (distinguishing between various layer-2 solutions and highlighting their unique features and impact on the end user).
109. *See* George Konstantopoulos, *supra* note 1 (discussing how optimistic rollups achieve faster and cheaper transactions by executing most transactions off-chain and only submitting a summary to the main chain).
110. *See Optimistic Rollups*, Ethereum Docs, *supra* note 20.
111. *See The Sequencer and Censorship Resistance*, Arbitrum Docs, *supra* note 5; *Shared Sequencing: Defragmenting the L2 Rollup Ecosystem*, Espresso Systems (HackMD), *supra* note 21; *What's the Difference Between Arbitrum Rollup and Arbitrum AnyTrust?*, Arbitrum Docs, *supra* note 57.
112. *See The Sequencer and Censorship Resistance*, Arbitrum Docs, *supra* note 5; *Shared Sequencing: Defragmenting the L2 Rollup Ecosystem*, Espresso Systems (HackMD), *supra* note 21.
113. *See* Kyle Charbonnet, *supra* note 2; *Shared Sequencing: Defragmenting the L2 Rollup Ecosystem*, Espresso Systems (HackMD), *supra* note 21 (emphasizing the challenges introduced by rollups, such as potential monopoly pricing, censorship, and fragmentation within the Ethereum ecosystem).
114. *See*, *e.g.*, *Shared Sequencing: Defragmenting the L2 Rollup Ecosystem*, Espresso Systems (HackMD), *supra* note 21 (discussing the benefits of shared sequencing, bridging between rollups, and atomic cross-rollup transactions).
115. *See Rollup Sequencers are Centralized: And That's Fine*, Blockworks, *supra* note 16 (emphasizing that while blockchain technology aims for decentralization, developers often resort to centralized mechanisms for efficiency and speed).
116. *See The Sequencer and Censorship Resistance*, Arbitrum Docs, *supra* note 5 (discussing how, despite the potential for sequencer misbehavior, rollup-2 protocols can be designed to ensure trustless security).
117. *See id*. (emphasizing the challenges introduced by potential sequencer misbehavior, like monopoly pricing, censorship, and fragmentation within the Ethereum ecosystem); Kyle Charbonnet, *supra* note 2; *Shared Sequencing: Defragmenting the*

L2 Rollup Ecosystem, Espresso Systems (HackMD), *supra* note 21 ("By relying on a single party for transaction ordering and inclusion in a rollup, they are prone to monopoly pricing and censorship."); *see*, *e.g.*, Sage Young, *supra* note 106 (reporting how the Arbitrum layer 2 went out of service for several hours due to a bug in the sequencer and a resulting transaction backlog that stressed the network).

118. *See Shared Sequencing: Defragmenting the L2 Rollup Ecosystem*, Espresso Systems (HackMD), *supra* note 21 (discussing the challenges of potential monopoly pricing, censorship, and fragmentation, and proposing shared sequencing protocols as a solution); *What's the Difference Between Arbitrum Rollup and Arbitrum AnyTrust?*, Arbitrum Docs, *supra* note 57 (demonstrating that regardless of the degree of centralization of sequencer operations, more crucial to maintaining the network's "trustlessness" nature is the decentralization of validators); *see also The Sequencer and Censorship Resistance*, Arbitrum Docs, *supra* note 5 (elaborating on the potential risks of a centralized sequencer and describing how Arbitrum maintains its claim to censorship resistance even if the sequencer misbehaves). Importantly, notwithstanding, the complexity of shared or distributed sequencing systems can potentially make it challenging for average users to understand, potentially hindering their trust in the network.
119. *See Rollup Sequencers are Centralized: And That's Fine*, Blockworks, *supra* note 16.
120. *Id*.
121. *See* George Konstantopoulos, *supra* note 1; *Layer 2: Ethereum for Everyone*, Ethereum, *supra* note 1.
122. *See Layer 2: Ethereum for Everyone*, Ethereum, *supra* note 1.
123. Notably, this is one of the primary objectives of the Cosmos network. *See* Cosmos Network, https://cosmos.network (last visited Aug. 24, 2023).
124. For example, a sequencer might neutrally exclude transactions based on built-in mechanisms meant to address risks and vulnerabilities and follow established user incentives.
125. *See*, *e.g.*, Off. of the Comptroller of the Currency, *Third-Party Relationships: Interagency Guidance on Risk Management*, OCC Bulletin 2023-017 (Jun. 6, 2023), https://www.occ.gov/news-issuances/bulletins/2023/bulletin-2023-17.html (promulgating guidance to federally regulated depository institutions on best practices in managing relationships with and use of third-party technology service providers); *see generally* Carl White, *Regulating Fintech: One Size Does Not Fit All*, Fed. Res. Bank of St. Louis: On the Economy Blog (Feb. 24, 2021), https://www.stlouisfed.org/on-the-economy/2021/february/regulating-fintech-one-size-does-not-fit-all (discussing how, when third-party financial technology providers provide services to a bank or its customers, there may be third-party risk management guidelines to which banks must adhere, such as auditing and monitoring their providers).
126. *See* Carl White, *supra* note 125 (emphasizing that the responsibility for meeting regulatory requirements for both in-house and outsourced technology needs falls on the banks that implement those technologies, not on the providers of those technologies).
127. Note that there may be many various, nuanced legal issues and related liabilities (such as in intellectual property, tort, contract, etc.) that are potentially implicated by any given blockchain protocol or software-based mechanism (like a sequencer) protocols. This chapter contemplates only broad legal principles and does not seek to address any particular legal or regulatory issues or classifications, under any theory, that may potentially be implicated by sequencers or other layer-2 rollup components.

Acknowledgments

The authors would like to thank Charles Lu of Espresso Systems, as well as DLx Law attorneys Lewis Cohen, Greg Strong, and Sarah Chen, for their valuable input and assistance in preparing this chapter. The authors would also like to thank industry participants and the project teams building the layer-2 blockchains referenced in this chapter, as well as general industry participants, who have greatly assisted them in their understanding of many of the underlying matters.

Angela Angelovska-Wilson
Tel: +1 202 365 1448 / Email: angela@dlxlaw.com

Angela is an early distributed ledger technology adopter and a leading authority in the evolving global legal and regulatory landscape surrounding distributed ledger technology and smart contracts. Prior to co-founding DLx Law, Angela served as the Chief Legal & Compliance Officer of Digital Asset and was part of the founding team. Prior to joining Digital Asset, Angela was a partner at Reed Smith where she regularly advised clients on the implementation of new technologies to finance and the complex regulatory schemes involved in the development, creation, marketing, sale and servicing of various financial services and products. Before Reed Smith, Angela spent most of her career in various roles at Latham & Watkins. Angela is a frequent public speaker on the topic of blockchain and the financial markets and has been recognized and ranked "Band 3" as one of the top-ranked lawyers in the blockchain space in the United States by *Chambers and Partners*.

Tom Momberg
Tel: +1 718 664 5458 / Email: tom.momberg@dlxlaw.com

Tom is an attorney at DLx Law, advising clients in an array of matters related to blockchain, decentralized finance, banking and payments systems, financial products, and financial technology applications. He joined DLx Law after working as in-house counsel for a payments and banking software service provider, advising on various legal and regulatory matters, risk, customer due diligence, and corporate best practices. Tom received his J.D. from George Mason University Law School in Virginia and his B.A. from the University of Wisconsin-Milwaukee. Tom is a former journalist, and, while in law school, he interned for DLx Law and served as a law clerk for several federal institutions in Washington, D.C., including the House Judiciary Committee, FCC, and CFTC.

Michael Mosier
Email: mm@arktouros.co

Michael is a co-founder of Arktouros PLLC legal boutique. He has twice been the first in-house counsel at emergent technology companies: Espresso Systems, developing a decentralized sequencer and configurable private computation, and Chainalysis blockchain analytics. He also is a partner in *ex/ante*, an early-stage venture fund investing in technology that advances democratic resilience and personal sovereignty. In public service, Michael was Acting Director, Deputy Director, and the first Digital Innovation Officer of the U.S. Treasury's Financial Crimes Enforcement Network (FinCEN). He also was Counselor (Cybersecurity & Emerging Technology) to the Deputy Secretary of the Treasury. Previously, he served as Associate Director and Acting Deputy Director of Treasury's Office of Foreign Assets Control (OFAC). Before Treasury, Michael was a Deputy Chief in the Department of Justice's Money Laundering Section and served at the White House National Security Council as a Director.

DLx Law
331 Park Avenue South, New York, NY 10010, USA
Tel: +1 212 994 6845 / URL: www.dlxlaw.com

Arktouros PLLC
1717 N Street NW, Suite 1, Washington, D.C. 20036, USA
URL: www.arktouros.co

Legal considerations in the minting, marketing and selling of NFTs

Stuart Levi, Eytan Fisch, Alex Drylewski & Dan Michael
Skadden, Arps, Slate, Meagher & Flom LLP

The increased popularity in recent years of people consuming and collecting digital content has presented a vexing problem; how does one establish that a certain version of a digital work is the "original" given that it can be easily and quickly replicated into identical copies? This problem also creates distinct challenges to developing a "digital ownership economy" in which consumers own a digital work (be it music, text, video, or graphics) as opposed to a "digital license economy" in which consumers license such works from a platform, and "lose" their works when their subscription terminates or the platform ceases to operate. The solution to this issue may lie with Non-Fungible Tokens (commonly known as "NFTs"), which can use blockchain technology to identify an original digital work, track its provenance, reward creators, and open up new business opportunities, such as by providing owners of an NFT unique access to digital or real-world content and experiences. Depending on the source, NFT sales in 2021 exceeded $25 billion to over $40 billion. The momentum continued through 2022 but has slowed in 2023 as the cryptocurrency industry has broadly faced headwinds compounded with a general economic downturn. This chapter describes what NFTs are and how they function, and provides an overview of some of the interesting legal issues and challenges that they present under U.S. law.

What is an NFT?

An explanation of NFTs might best start with the somewhat unusual name used to describe these digital ownership markers. In general, when blockchain technology is used as a means to generate coins or tokens, the resultant digital assets are "fungible," meaning that they are identical and interchangeable 1:1. For example, each Bitcoin is identical to all other Bitcoins. Fungible tokens would therefore be ill-suited as a means to identify and distinguish an "original" digital work. As its name implies, the idea behind "non-fungible" tokens is to generate tokens that are unique, thereby enabling one to use these tokens to identify a digital good as the original or one of a limited series of originals. "Tokens" are also somewhat of a misnomer, as NFTs are actually pieces of computer code, known as smart contracts, that reside on blockchains and include "metadata" that, among other fields, includes: an NFT's unique ID; a short description of the work associated with the NFT; and, in most cases, a pointer to an off-chain location where the work associated with the NFT is stored.[1]

Various stakeholders, including creators, rights holders and brands, have exploited NFTs in different ways in a number of different sectors. As the NFT market has grown and evolved, we have seen that most NFTs generally fall into one or more of the following categories.

Digital art

In its simplest form, NFTs are associated with digital works created by artists. This has ranged from artists who are just getting started in their careers and can use NFTs as a means

to connect directly with potential fans and collectors, to well-known digital artists who already have significant followings. The growing market for art NFTs has led the major auction houses to embrace this space and create their own NFT divisions.

Fan engagement and collectibles

Traditional intellectual property rights holders, including entertainment companies and sports leagues, are using NFTs to create and market digital collectibles as a means to build fan engagement both for existing and potentially new fans. This has included everything from pure collectibles to digital cards featuring game moments and clips that can be used for fantasy leagues.

In the music industry, NFTs are being used by artists to connect directly with fans by selling new music or merchandise. For example, a never-before-heard demo recording of Whitney Houston at age 17 was auctioned for $999,999, and in March 2022, rapper Snoop Dogg released a set of songs as an NFT mixtape on OpenSea.[2] In December 2022, DJ Armin van Buuren released a collection of digital art NFTs that grant token-holders early access to unreleased music, access to fan meetup events and monthly giveaways.[3]

Gaming

Both new and legacy gaming companies are looking at ways NFTs can be implemented to allow players to own in-game assets that they purchase and potentially transfer those assets in other games. This ownership structure would also allow players to sell, trade, and even rent out in-game assets that they have acquired.

PFP project NFTs

"Profile Picture" or "Picture-as-Proof" NFT initiatives typically involve the minting of thousands of NFTs at once of characters (e.g., animated pandas, apes, cats), often algorithmically generated with slightly different traits or attributes (e.g., wearing a different hat or expression). Owners of the NFTs associated with these graphic images can typically interact with a custom-built environment or community and unlock certain user experiences.

Brand-driven NFT projects

Retail brands have also embraced NFTs as a means to engage with their consumer base more directly and more deeply. These NFTs can be digital versions of the brand's products or other types of collectibles. The NFTs can "reward" consumers of legacy products, promote new products or services, or raise awareness for, and help fund, certain charitable causes. In some cases, these NFTs grant holders early access to product benefits, access to a community discussion forum, or the ability to participate in live or virtual experiences.

Future uses

As the potential use cases for NFTs continue to develop, a number of projects are experimenting with using NFTs as a source identifier for both tangible and intangible goods and services. This might include school transcripts and professional certificates, proof of identity, and ways to record ownership of specific assets.

Key stakeholders in the NFT market

There are a number of stakeholders in today's NFT sector:

- *Technology Providers*. There are numerous technology providers that provide services to clients related to minting, developing, storing and selling NFTs. Such providers can create white-labelled platforms or storefronts for clients looking to create their own NFT offerings and marketplaces.

- *Marketplaces*. NFTs are commonly purchased and sold through marketplaces. Some of the marketplaces only offer "curated" content in which the marketplace vets the individual digital creator who wants to list their works for sale, or has written agreements with large rights holders (e.g., a sports league or team, an entertainment company). Other marketplaces merely provide open platforms in which anyone can post an NFT for sale. Finally, some marketplaces provide both a "curated" and an "open" section.
- *Creators and Rights Holders*. As has been noted, NFTs are typically being developed and minted by individual creators or by larger rights holders.
- *Owners of NFTs*. The owner of an NFT, which is typically an individual, but could also be a Decentralized Autonomous Organization ("DAO").[4]

Technology background

In order to understand the legal issues raised by NFTs, it is important to understand some of its technology underpinnings. NFTs are bought, sold and transferred on blockchains. A blockchain is a peer-to-peer decentralized network of computers that allows for transactions to be transparently recorded.[5] Blockchain transactions are also transparent such that anyone can observe all transfers of an asset from its point of creation, with each participant represented on-chain by their blockchain address (a string of alphanumeric characters). Because each block of transactions on a blockchain is cryptographically based on the previous block, blockchains are immutable; meaning that for all practical purposes, historical records cannot be altered or deleted. A blockchain therefore provides a compelling technology solution to creating and perpetually storing immutable digital certificates of ownership that can be tracked from their creation or "minting."

Although NFTs enjoyed mainstream adoption starting in late 2020, the idea of NFTs on a blockchain dates back to 2014. They became more widely adopted within the blockchain community in 2018 with the release of a common standard (ERC-721) for NFTs minted on the Ethereum blockchain.[6] While Ethereum remains a popular blockchain for minting and storing NFTs, other blockchains that sometimes offer increased transaction speeds and lower transaction costs have gained traction, thereby expanding the options for NFT issuers. In addition, "Layer 2" protocols have proliferated, which essentially function as blockchain networks that overlay and are connected with underlying "Layer 1" networks. Typically, transactions can be bundled on Layer 2 and then recorded on Layer 1, offering potential scalability solutions to problems such as congestion, and high gas fees, on Layer 1. Technological developments are also fueling new developments in NFT adoption. The Ethereum standard ERC-1155 allowed a developer to combine the token standard for fungible tokens (ERC-20) and NFTs (ERC-721) in a single smart contract. This enabled the efficient transfer of multiple different fungible tokens and NFTs in a single transaction, thereby facilitating faster network speeds and lower transaction costs for participants. A proposal for ERC-6551 will assign Ethereum smart contract addresses to NFTs. These token-bound accounts will allow NFTs to perform transactions, hold assets and interact with applications, spurring novel future use cases for NFTs.

A key technological development in 2023 was the introduction of NFTs on the Bitcoin blockchain. While the Bitcoin blockchain does not offer the same range of functionality as the Ethereum blockchain, developers were able to replicate the NFT experience on the Bitcoin blockchain through the use of "ordinals." The ordinals protocol allows individual satoshis, the smallest unit of Bitcoin currency, to be assigned a unique identifier and transacted, including with additional data such as images or video appended.[7] This unique

identifier meant that satoshis could be treated as non-fungible digital assets, along with the image or video attached to them, thereby creating an NFT ecosystem on the Bitcoin blockchain. A critical feature of ordinal NFTs is that, in contrast to NFTs on most other blockchains, the actual NFT content is itself stored on-chain, thereby eliminating a number of risks with other blockchains where storage on-chain is not feasible and content is stored in an off-chain location and made available via a pointer in the NFT metadata.

A key market feature of NFTs results from the fact that it is a programmable piece of computer code. This allows developers to include, for example, a programmable royalty (or resale) function that automatically transfers a specified amount of cryptocurrency from the sale price of an NFT to the on-chain wallet of the one or more creators, rights holders, or participants in a project each time an NFT is sold on-chain. This technology opens up numerous new opportunities to reward those involved in an NFT project. There is a royalty payment standard (ERC-2981) that standardizes the manner of signifying royalty information in ERC-721 tokens, but it still has its limits, as all parties to the transaction are still required to honor and enforce the royalties. Due to the current lack of standardization for programmable royalties, typically NFT marketplaces are required to overlay additional smart contracts at the platform level to facilitate the collection and distribution of royalties. As a result, there may be inconsistencies with respect to how royalties are collected across platforms and uncertainty as to whether royalties will be honored as NFTs are transferred across platforms. In 2022, competition among NFT marketplaces generated a trend towards marketplaces enforcing limits on royalties or announcing either that they will not honor royalties or that royalties are optional for NFT purchasers to pay. In response, certain NFT issuers and marketplaces blocked resales of NFTs on marketplaces that do not honor royalties.

Legal issues presented by NFTs

The widespread adoption of NFTs has raised a number of interesting questions under U.S. law, some of which are traditional legal questions that arise in the creation of any creative work, and some that are questions of first impression.

Who has the right to mint an NFT?

Copyright considerations

Anyone minting an NFT, be it an individual creator or a rights holder with a library of intellectual property assets, will need to determine whether they have the appropriate rights to do so. Given that NFTs have only been adopted as a means of identifying digital goods in recent years, it comes as no surprise that many contracts involving the creation of, and rights to, digital goods – be it art, music, memorabilia, or other goods – make no reference to who owns the right to create or "mint" an NFT associated with the digital good. While clauses addressing NFT rights may be added to many such agreements (as discussed below), until that point, those analyzing who has the right to mint an NFT must rely on a standard intellectual property analysis and also look at whether there are clauses in agreements that could be construed to sweep in NFTs.

Under U.S. copyright law, a creator owns the copyright in a creative work upon the creation of that work and its fixation in tangible form, regardless of the medium. The copyright holder enjoys a "bundle of rights" with respect to the work, including the exclusive right to reproduce, prepare derivative works of, publicly perform and publicly display the work.[8] This "bundle of rights" can be held or licensed by the copyright holder in whole or in part, but critically, unless each of the rights are expressly assigned or licensed away, they will remain with the creator, or, in copyright parlance, "author," of the work.[9]

Those minting an NFT will also need to take into account whether there are joint authors who have applicable legal rights that could impact the minting of an NFT. The issue of what constitutes joint ownership is nuanced, and those minting an NFT will want to understand who might be able to claim they have a joint ownership right in a work.

Musical works present their own unique set of issues. Generally, each piece of recorded music has a compositional copyright in the music itself (the musical composition and lyrics) and a master copyright in the sound recording that is the particular expression of the composition, as created by performing or recording artists. The master rights are held by the artist or, more typically, by a label. If a third party wants to create a derivative work of a composition or a master recording by combining a musical work with a video clip, they will require a "sync license" to use the composition and a master use license to use the master recording. Creating an audio-only recording of a composition requires a "mechanical license." Depending on the circumstance, performing the composition may require a "public performance" license.

Given the foregoing, it is not clear where this leaves a party seeking to mint an NFT of a digital work. Where a party seeking to mint an NFT holds the entire bundle of copyright rights, this is a non-issue. However, in cases where the bundle of rights has been dispersed among multiple parties, including through exclusive license arrangements, the answer may be less clear. Minting an NFT often requires at least some exercise of copyright rights: for example, a digital work linked to an NFT is generally displayed by the seller, such as on a marketplace, so that the purchaser knows what they are acquiring. Video clips and music offered as NFTs may trigger performance rights. In most cases, the parties will need to look back at agreements that memorialized the allocation of rights to determine who can authorize the creation of an NFT, keeping in mind that this might entail approval from multiple parties. These parties will also need to consider the commercial terms of these arrangements. For example, many agreements concerning creative works include broad "sweep" clauses, such as a broad right to "commercialize" a work or exploit a work in connection with future technologies. Whether such clauses can be interpreted to include the right to mint NFTs will require a case-by-case analysis, although courts have interpreted these clauses to include new technologies.[10]

Those seeking to mint or exploit an NFT must also consider the moral rights of the author of the associated work. The scope of moral rights will depend on the applicable jurisdiction, but generally will protect certain non-economic rights of the author. While, in the United States, such rights are limited to visual works under the Visual Artists Rights Act of 1990 ("VARA") and extend only to right of attribution and integrity, in other jurisdictions, moral rights may include an author's control over whether and in what way their work is displayed and how it is used.[11] Whether an author can seek to invoke their moral rights to prevent the creation of an NFT associated with their work remains to be seen, but is an issue that should not be discounted.

Many NFT marketplaces seek to protect themselves from issues of copyright ownership by requiring those minting NFTs to represent that they have the appropriate rights, and by disclaiming any liability to purchasers if that proves not to be the case.

Two cases in the NFT space illustrate these copyright issues. In June 2021, Roc-A-Fella Records, Inc. ("RAF") sued Damon Dash (a co-founder of RAF) after Dash's alleged attempt to auction off the copyright to Jay-Z's debut album, *Reasonable Doubt*, as an NFT. RAF argued that the album and its copyright were assets belonging to RAF, and Dash could not sell such rights as an NFT or otherwise. The parties settled in June 2022. In late 2021, Quentin Tarantino launched an NFT collection of digital images of his handwritten

screenplay for *Pulp Fiction*. Miramax, which owns the copyright to the film, sued Tarantino, alleging copyright infringement on the basis that Tarantino had sold Miramax those versions of his screenplay as well, and therefore did not have the rights to mint NFTs to the screenplay. Miramax highlighted the catch-all language in its contract with Tarantino that stated it owned "all rights . . . now or hereafter known. . . in all media now or hereafter known." The parties settled the lawsuit under terms that were not disclosed.

Trademark considerations

Those minting NFTs also need to be aware of issues surrounding trademarks (to the extent incorporated into an NFT without the permission of the trademark owner) and rights of name, image and likeness ("NIL rights").

Both the Lanham Act and corresponding state laws provide protection against the unauthorized use of trademarks in a manner that is likely to cause confusion among consumers.[12] Moreover, the use of any name, symbol, image, or device that is likely to cause mistake as to the source, affiliation, or sponsorship of a good or service is also prohibited.[13] Accordingly, the use of trademarks or colorable imitations of trademarks in NFTs may implicate a third party's trademark rights. Moreover, if the underlying trademark is famous and distinctive, rights under the state and federal dilution statutes may be implicated.

A few NFT-related lawsuits highlight the unique trademark issues that can be presented by NFTs. In 2021, luxury brand Hermès sued Mason Rothschild for minting and selling "MetaBirkins" – NFTs of faux-fur digital renditions of the classic Hermès Birkin handbag – alleging that Rothschild infringed on the company's trademarks. Rothschild claimed that MetaBirkins are a form of artistic expression and protected as free speech under the *Rogers v. Grimaldi* test.[14] According to the test, artistically expressive uses of trademarks may be protected by the First Amendment, and therefore do not constitute trademark infringement "unless the [use of the mark] has no artistic relevance to the underlying work whatsoever, or, if it has some artistic relevance, unless [it] explicitly misleads as to the source or the content of the work."[15] In May 2022, the court denied the parties' cross-motion to dismiss. In February 2023, in the midst of trial, the court issued a formal opinion clarifying its position, noting that the *Rogers* test applied to the case and instructed the jury to assume that the MetaBirkins were, in at least some respects, works of artistic expression and that Hermès was required to establish, by a preponderance of the evidence, that Rothschild's use of the trademarks was "intentionally designed to mislead potential consumers" into believing Hermès was associated with the project.[16]

The jury ultimately sided with Hermès in January 2023, finding that Rothschild was liable and not shielded by the First Amendment. The dispute was closely watched for its potential to set precedent on the application of trademark law to NFTs; however, the fact that the MetaBirkins were linked to NFTs ultimately proved not to be dispositive to the jury's decision-making. Hermès argued that Rothschild's use of the "BIRKIN" mark referred to and promoted the tokens themselves, which held value separate and apart from any associated images that may be protected artistic works. However, Judge Rakoff found undisputed evidence in the record that consumers understood they were purchasing exclusive ownership of the digital image associated with the NFT and were not viewing the token purchase as separate from the digital image purchase. He also reasoned that, because NFTs are simply code pointing to where a digital image is located, such an associated digital image does not automatically turn into a commodity without First Amendment protection. However, the court's rationale should not be taken to mean that all digital images associated with an NFT are *per se* protected by the First Amendment, as in a footnote in the May 2022

order, the court noted that Rothschild appeared to concede that the *Rogers* First Amendment protection may not apply if NFTs were attached to a digital image of a virtually wearable Birkin bag; in such a case, the use of the MetaBirkins mark would refer to a non-speech commercial product.[17]

In June 2022, Yuga Labs, the creator behind the Bored Ape Yacht Club ("BAYC") NFT collection, sued Ryder Ripps and additional defendants for their use of the BAYC trademarks in connection with the marketing and sale of their "RR/BAYC NFT" collection, which are allegedly identical copies of Yuga Labs' Bored Ape NFTs. Yuga Labs asserted that the defendants used the BAYC trademarks and logos to promote their infringing RR/BAYC NFTs and intentionally misled consumers into believing that the infringing NFTs were legitimate. Yuga Labs claimed common law trademark infringement, false designation of origin and false advertising under the Lanham Act, among other claims, and seeks injunctive relief to bar defendants from using the BAYC trademarks, as well as monetary relief. The court decided in Yuga Labs' favor in April 2023, by granting Yuga Labs' motion for summary judgment with respect to its common law trademark infringement, false designation of origin, and cybersquatting claims. Notably, the court rejected Ripps' argument that the RR/BAYC NFTs should be protected as First Amendment artistic expression under *Rogers*, noting that the "[d]efendants' sale of RR/BAYC NFTs [was] no more artistic than the sale of a counterfeit handbag, making the *Rogers* test inapplicable."[18]

Right of publicity considerations and the evolution of intellectual property rights

Those minting NFTs also need to be aware of issues surrounding rights of name, image and likeness ("NIL rights"). Incorporating an individual's NIL likeness into an NFT without authorization risks infringement of that individual's right of publicity. The right of publicity is a right protected by state law. It gives an individual the exclusive right to control the commercial use of his or her persona, meaning one's NIL. Over 35 states currently recognize an individual's right of publicity. Although the scope of protection varies across jurisdictions, infringement typically occurs when a third party exploits the subject's likeness for a commercial purpose without permission.

In January 2022, rapper Lil Yachty filed a lawsuit against Opulous and Ditto Music for alleged malicious use of his name and likeness in connection with Opulous' NFT project, which ultimately raised over $6.5 million in venture capital funds. In his complaint, Lil Yachty alleged that he did not receive any financial benefit from the raise, despite use of his likeness. The parties ultimately settled in April 2023.

One can expect that the application of traditional concepts of intellectual property law to NFTs will continue to evolve, especially as NFTs expand into the developing "metaverse" and gaming industries. In July 2022, in response to a letter from two members of the Senate's intellectual property subcommittee, the U.S. Copyright Office and the U.S. Patent and Trademark Office announced that they will conduct a joint study to examine intellectual property issues related to NFTs to provide legal clarity amid rising questions and legal disputes centered around this technology.[19] In January and February 2023, the offices held public roundtables and collected public comment in furtherance of its joint-study efforts.

In January 2023, the Nice Classification, an internationally recognized system used to classify goods and services for the registration of trademarks and service marks, provided guidance with respect to the classification of goods and services related to digital assets. Specifically, a few of the classifications were updated to include references to blockchain-based digital assets, such as NFTs, as well as metaverse activities and cryptocurrencies. This is anticipated to provide clarity for practitioners looking to register trademarks in connection with these activities.

In addition to providing guidance to practitioners, additional regulatory clarity may help resolve the intellectual property disputes in this space and provide participants with guidance as they navigate unchartered waters.

Incorporating NFT rights into agreements

Whenever a new technology is introduced, ranging from CD-ROMs to streaming, there is always a rush to incorporate that technology into the grant of rights sections of agreements. One can expect similar treatment of NFTs in a variety of agreements, such as: freelance agreements; agreements pursuant to which a copyright holder grants rights to a third party to exploit or commercialize their work; and agreements between talent (e.g., musicians, actors, athletes, or influencers) and an agency or representative. However, merely adding "NFTs" to a litany of rights will likely fall short of addressing the underlying complexities of what NFT rights actually mean, where the NFT and associated content will be stored, and the growing number of ways NFTs can be structured. Contractual obligations to use commercially reasonable efforts to police and enforce a rights holder's intellectual property rights are also more complicated in the context of NFTs, given, as discussed below, the limited ability to take down unauthorized or infringing works linked to the NFTs. The parties will also want to consider the inclusion of blockchain-specific disclosures and risk factors.

If a licensor seeks to grant a licensee rights to mint an NFT, explicit language should be included that outlines the scope of rights and the parameters of the minting (i.e., is all of the intellectual property or only a subset permitted to be minted; is there a limitation on the type of marketplace used; will only one NFT be permissible per work or could there be a limited supply (i.e., five originals, much like how there may be multiple limited editions of a print); what rights can the licensee grant to purchasers of the NFT; can an NFT subsume assets that are outside the scope of the agreement, etc.). This will ensure that the licensor does not inadvertently grant overly broad rights that do not align with its objective and will help to avoid issues of breach of contract or infringement down the road.

Issues of persistence

Critically, while an NFT is stored on a blockchain, in most cases the work associated with the NFT is not (i.e., it is "off-chain"). This is because most blockchains are programmed to assess a fee (known as a "gas fee") for storing or transferring files, and for the large files that comprise most digital works associated with an NFT, that cost would be prohibitive. Instead, most NFTs include a metadata field with a pointer or link to an off-chain resource where the associated work is stored. Thus, while the NFT might itself be immutable, the off-chain work may not have that same persistence. For example, an NFT might include a pointer to an online location, such as a URL, where the underlying work can be observed. The risk of location-based pointers is that the file at that location could be changed, much the way a website can change from one visit to the next. In a well-publicized case, a digital artist known as "Neitherconfirm" highlighted this persistence issue by changing the computer-generated portrait images associated with the NFTs the artist had sold on the OpenSea NFT marketplace into photos of carpets (simulating a scam known as a "rugpull").

One solution is to use file storage systems that rely on content identification, instead of location-based pointers, such as the InterPlanetary File System ("IPFS"), a peer-to-peer distributed file system. In a content identification system, files are identified through a Content ID (a cryptographic "hash" of the content) as opposed to where the file is located. If someone sought to modify the digital work, the modified work would generate a new Content ID, while the original file linked to the NFT would remain. While systems like

IPFS are superior to location-based systems for NFTs, there is not necessarily a guarantee that a work will exist forever. While IPFS is designed for multiple computers to hold a copy of a work, if there is only one copy on IPFS and it is being stored by one particular computer that goes out of business, that work could be lost.[20] In addition, for data to persist on IPFS, it must be "pinned" to a node. Third-party pinning services run multiple IPFS nodes and allow users to upload, pin, and retrieve data from such nodes for a fee. If the user stops paying for the third-party pinning service, the uploaded data may be lost entirely.

An NFT is therefore only as valuable as the persistence of its underlying work. For NFT purchasers this is a commercial risk issue. For creators, rights holders, and NFT marketplaces, persistence is an important technical point that may affect a myriad of provisions in NFT-related agreements, such as risk factors to be disclosed and limitations on, or disclaimers of, liability.

The issue of persistence becomes particularly important for rights holders if the platform on which their NFTs are marketed ceases to operate. Rights holders will want to make sure in their agreements that they have the right to take over the storage of the NFTs. This may involve contractually requiring the counterparty to update the metadata for the NFTs such that the pointer in the NFTs resolves to a different location, such as a proprietary server where the rights holder is hosting the images. Alternatively, rights holders can ensure that they have the right to take over the servers on which the works are stored, either through taking over physical control, or more likely, taking over the contract governing the use of that server. In the case of works stored on IPFS, rights holders may want to make sure the work will continue to be preserved if the now-defunct platform was hosting the work on its own gateway. While rights holders could mint new NFTs for their works and provide them to then-current NFT holders, such a solution would defeat one of the fundamental benefits of an NFT – demonstrating its provenance from when it was first created.

Issues of authentication

A common misconception is that an NFT automatically provides an immutable certification of authenticity. In reality, while an NFT allows one to view the blockchain address of its original creator, some independent means of verification is required to know that the person or entity associated with that address is who they claim to be or had the appropriate rights in the associated work. This may require direct interaction with the minter of the NFT (a solution that may not be scalable) or use of a trusted third party to authenticate that party. In all cases, those within an NFT ecosystem need to be cautious about explicit claims or legal representations of "authenticity."

What rights are being acquired in the underlying work?

Purchasing an NFT does not provide the purchaser with intellectual property rights, particularly copyright rights, in the associated work. As noted above, under U.S. law, the "bundle of rights" is held by the author of a work unless they are expressly assigned or licensed away. In this respect, purchasing an NFT is no different from purchasing a piece of physical art. While the purchaser of a painting or sculpture may own the physical work, they typically do not acquire any intellectual property rights in such work (e.g., they cannot create and sell posters of the painting they purchased).

The rights that an NFT purchaser receives are therefore generally governed by the license provided by the marketplaces that offer the NFTs for sale. That could be general terms that apply unilaterally to all NFTs offered for sale on the marketplace or bespoke license rights that apply to the works of individual creators or rights holders.

Most current marketplaces grant an NFT purchaser a non-exclusive and non-transferable license to use, copy and display the creative works underlying the NFT for personal use. For example, some marketplaces provide a limited license to display the work solely to promote the purchaser's "purchase, ownership, or interest" in the underlying work (e.g., through social media), promote discussion of the work, display the work on third-party marketplaces or exchanges to sell or trade the NFT, or display the work within decentralized virtual environments. In the instance where the marketplace terms of use are silent on license rights, the NFT purchaser would likely not have any intellectual property rights in the creative work, and would likely only have an implied license to display the work for personal use. In the early days of the NFT boom, the right to commercialize works associated with NFTs was expressly carved out or was allowed for only limited purposes. For example, Dapper Labs, the company behind the early-stage CryptoKitties NFTs and NBA Top Shot, proposed a form of NFT license for the industry to use (NFT License 2.0) that would allow a purchaser to commercialize a work up to $100,000.[21] Yuga Labs was one of the first projects that granted NFT holders the right to commercialize the creative work linked to the NFT; each Bored Ape NFT holder was granted a license to use the underlying art for the purpose of creating derivative works, such as merchandise.[22] BAYC triggered a wave of NFT projects that granted similar commercialization rights and, over time, many NFT projects have opted to grant purchasers even broader permitted commercialization rights.

The typical NFT terms and conditions also set forth certain restrictions on how the creative work underlying the NFT may be used. For example, a number of license agreements prohibit use of a creative work in connection with media that depicts hatred, intolerance or violence, or that otherwise infringes upon the rights of others.

Given that the purchaser of an NFT is typically getting a license to the work associated with the NFT, each NFT sale therefore has two components: the "sale" of the actual NFT (which the purchaser owns outright); and a limited license to the work. The distinction between a sale and license can have important ramifications under U.S. law.

Under the first sale doctrine, the "owner of a particular copy" may "sell or otherwise dispose of the possession of that copy" without the authority of the copyright owner.[23] For example, one may resell a physical book they purchased without infringing the copyright holder's distribution right. "Once the copyright owner places a copyrighted item in the stream of commerce by selling it, he has exhausted his exclusive statutory right to control" the distribution of that particular item.[24] Purchasers of NFTs may conclude that this doctrine provides comparable rights with respect to NFTs. However, the U.S. Copyright Office and at least one court have concluded that the first sale doctrine does not necessarily apply to digital works.[25] The rationale is that the first sale doctrine is only a narrow exception to the right of distribution. However, when a digital work is transferred, a new copy is electronically created, thereby infringing on the copyright owner's exclusive right to make copies. In addition, the first sale doctrine does not apply to works that have been licensed, as opposed to sold.[26] Creators and rights holders should therefore be careful to clarify that while a purchaser may be *buying* the NFT, they are only *licensing* the associated digital work.

Whether terms and conditions "travel" with an NFT

When NFTs are first minted and offered for sale or otherwise distributed, there are several ways the NFT creator or issuer may grant rights, or purport to grant rights, in the underlying artworks to NFT purchasers, assuming they themselves have the appropriate rights to do so. Most often, NFT issuers make the NFTs available for initial sale or distribution through the issuer's own website platform or a platform offered by their business partner. In these

cases, the NFT issuer can rely on a "click-wrap" agreement pursuant to which purchasers must affirmatively "click" to agree to the applicable terms and conditions in order to obtain an NFT. Alternatively, the NFT issuer might include a link to the terms and conditions on the website hosting the initial launch (often on the bottom of the page) that the user is not directed to review, let alone affirmatively agree to, prior to purchasing the NFT. These "browse-wrap" agreements sometimes state that mere use of the website constitutes assent to the terms and conditions. In other cases still, commercial rights are granted through posts to online NFT-community fora (such as Twitter or Discord) or through an FAQ or roadmap on the NFT issuer's website.

To determine whether such terms and conditions are binding on the initial purchasers of an NFT, the same analysis would be used that has traditionally been applied to online contracts. Courts consider whether purchasers (i) were on notice of the terms, and (ii) actually or implicitly assented to them.[27] Applying this framework, courts generally enforce click-wrap agreements because they require purchasers to physically manifest assent (e.g., clicking an "I accept" button that explicitly indicates assent to the terms of use).[28] In contrast, since browse-wrap agreements do not require explicit physical assent, courts typically will only find them enforceable if they are presented in a clear and conspicuous manner.[29] This can be a high bar, as courts have refused to enforce terms placed on a submerged screen,[30] located exclusively at the bottom of a website,[31] situated among many other links,[32] or even in a link included on every page of a website near other relevant user prompts.[33]

The Ninth Circuit's recent dicta in a concurring opinion in *Berman v. Freedom Financial Network, LLC* about the enforceability of different online contracts is instructive. There the court found that the font size and format of a website's contractual terms were not conspicuous enough for a reasonable consumer, and that clicking a large green "continue" button placed near these terms did not manifest unambiguous assent.[34] Guided by two internet contract formation cases decided by the California Courts of Appeal,[35] the concurring opinion took the analysis further, asserting that, under California law, click-wrap and scroll-wrap agreements (i.e., agreements where users must physically scroll to the bottom to click an "I accept" button) are presumptively enforceable,[36] while browse-wrap agreements are *per se* unenforceable.[37]

Thus, simply placing the terms and conditions that apply to an NFT, including any commercial rights being granted, on a link accessible at the bottom of the NFT issuer's website may not bind the initial NFT purchaser in all cases. Similarly, folding terms and conditions into the registration process for an NFT purchase or "allow list" (i.e., pre-registering for access to purchase NFTs) through a sign-in wrap agreement does not necessarily give rise to an enforceable contract in all jurisdictions. General online statements in social media or in FAQs, without more, may also not be enforceable. The issue with granting rights through social media statements is also exacerbated by the fact that, in many cases, the poster of the statement may not have the authority to even grant such rights (e.g., a third-party moderator on an NFT issuer's channel).

The issue of whether terms and conditions are binding on the owner of an NFT becomes far more complicated with respect to downstream purchasers of NFTs. To the extent a purchaser is buying an NFT on the same marketplace where it was first sold, there should be no issue in assuming that the future purchaser has also agreed to be bound by the marketplace's terms. However, one of the strengths of NFTs is that they are often transferable outside of the platform where they were first offered. In these situations, a future purchaser may not be aware of the license terms and restrictions that attach to the associated work. That is because there currently is no effective and generally accepted mechanism for legal terms to

"travel" with an NFT. While secondary marketplaces typically have their own terms and conditions, these relate to the use of the marketplace, not the individual NFT. Thus, even assuming the best-case scenario where the initial purchaser agreed to the terms through a click-wrap or scroll-wrap agreement, it is far from clear how a downstream purchaser would be aware of, let alone agree to, the terms of such an agreement.

To date, there have been a number of approaches to address this issue, each of which presents its own shortcomings, and none of which have been universally adopted. Including a link to the license terms of the metadata of the NFT may not solve the issue since the purchaser may not look at the metadata before making a purchase, and even if the purchaser did, the NFT sale/transfer process may not include a step where the purchaser manifests their assent to the terms. Some companies are developing technology solutions where an NFT is "wrapped" in a legal agreement to which the purchaser must consent before the NFT can be transferred. However, such a solution would require widespread adoption and implementation across platforms to effectively ensure that terms and conditions are traveling with the NFT as it transfers between platforms.

Enforcement by rights holders

New technologies to commercialize intellectual property rights also inevitably yield cases of infringement and piracy, and NFTs are no exception. Companies with robust intellectual property libraries may want to push out statements that any NFTs associated with their properties are unauthorized unless originating from the company, and educate their employees and freelancers about whether they have the right to mint NFTs of works they created for the company.

If an NFT is minted without the authority of the rights holder, the rights holder likely has a claim for copyright infringement, since a number of their exclusive rights would have been violated (e.g., the right to copy, distribute, display, and perform the work). However, enforcing even clear claims of infringement may be challenging in a decentralized ecosystem where identifying the infringing party may be difficult. A rights holder may have the most success focusing on the centralized touch points of the ecosystem, such as NFT marketplaces. Many NFT marketplaces allow copyright holders to submit take-down notices under the Digital Millennium Copyright Act ("DMCA") if they believe their work is being infringed by NFTs available on such marketplaces.[38] However, a successful take-down likely only means that the NFT listing and images of the work displayed on the marketplace will be removed. It does not mean that the infringing work will be deleted from whatever platform or server it may be stored on. It also means that if the NFT has been sold already, the NFT likely still exists in the wallet controlled by the owner of the NFT, as the marketplace would have no ability to access that NFT. The rights holder would need to seek to take down the work from the system it is stored on, which leads to another complicating factor when applying the DMCA to NFTs.

As discussed above, the digital work associated with an NFT may be stored in a variety of different ways. In some cases, the marketplace may store these works on its own proprietary servers or may store them on the servers of a cloud provider. In these cases, the marketplace could take the additional step of removing the infringing work from the storage system it owns or controls. However, if the digital work is stored on a decentralized file system, such as the IPFS file storage system, as noted above, there are limited practical ways for a copyright owner to track down each server where an infringing work might be stored and get it taken down. The IPFS file storage system, for example, includes its own DMCA take-down process, but a rights holder would need to approach each IPFS "gateway" and have them take down the infringing work.

Importantly, while a DMCA take-down notice may result in removal of displays of work or even removal of the work itself, the NFT itself will likely remain given the immutability of blockchains. However, rights holders may take some comfort in the fact that an NFT pointing to a work that has been removed will likely have little value.

The DMCA also provides a mechanism for a rights holder to serve a subpoena along with its take-down notice that requests certain identifying information about the infringer.[39] Such a subpoena may prove to be a useful tool in the blockchain context.

In some cases, a rights holder may have a claim against the marketplace for contributory infringement if it can show that the marketplace was aware of the infringing activity, and induced, caused, or materially contributed to the infringing activity.[40] Given the active role that many marketplaces play in the minting and offering of NFTs, the second prong could be easy to establish.[41] However, most NFT marketplaces are likely unaware of infringing activity taking place on their platforms. In order to establish knowledge, a plaintiff would need to demonstrate knowledge of "specific infringing material" that is available to purchasers.[42]

Remedies for NFT purchasers

In the event that a work associated with an NFT is taken down due to copyright infringement or otherwise, the remedies that may be available to the then-current NFT owner may be significantly limited. As an initial matter, locating the person or entity that minted the infringing NFT may be difficult if the person or entity that minted the infringing NFT is only identifiable through their blockchain address, since blockchains only list alphanumeric public keys of blockchain participants and the person could be located anywhere in the world. In addition, most NFT marketplaces are careful to disclaim any liability for the authenticity or legitimacy of the NFTs offered on their sites and make abundantly clear that the purchaser is acquiring the NFT at their own risk. Some marketplaces, such as those that curate the creators whose works they offer, have mechanisms in place to try and minimize the risk on the purchaser.

A purchaser's strongest claims may be in cases where they are able successfully to assert that they were misled by the marketplace or rights holder. Clear disclosures of any limitations on the purchaser's right, and clear disclosure of any fees or resale royalties that may be extracted from any future sale, are essential.

Disclaimers of liability

NFT marketplaces, like most providers of services matching sellers and buyers, disclaim any liability in connection with providing the platform. Additionally, marketplaces will typically disclaim any liability in connection with the ability to use, access, or transfer the NFTs themselves.

The terms of use commonly state that the marketplace, as well as the NFTs, are made available on an "as is" and "as available" basis and the provider makes no warranties that the marketplace or NFTs will be available on an uninterrupted basis or that they will be accurate, reliable or safe. Purchasers should also expect that the platform providers will not guarantee that the marketplace or NFTs will be free of viruses or other harmful components.

In addition to stating that the marketplace and NFTs are provided on an as-is basis, NFT marketplace or platform providers often apprise the user of a number of disclosures and risk factors, many of which are unique to blockchains. These disclosures may cover, for example:

- the risk that bad actors may hack or exploit systems and steal NFTs or may otherwise act in a malicious manner;
- the risk that NFTs may compete with other digital assets, and this competition may negatively impact the price of NFTs;

- the risk that the business or organization issuing the NFTs may declare bankruptcy or cease operations;
- the volatility of blockchain and digital assets, and that the market for NFTs is new and volatile and the price of NFTs may decrease over a short period of time;
- the uncertainty of tax treatment for NFT transactions;
- clarification that the platform provider does not store, send or receive the NFTs, and that this takes place on a blockchain the platform might not control;
- risks that the asset associated with the NFT may become inaccessible;
- risks arising from a hard fork in the blockchain on which the NFT is stored;
- risks arising from the uncertain regulatory environment surrounding blockchain technologies and cryptocurrencies, including legislation or regulation that could be adopted that negatively impacts the use, transfer, exchange or price of NFTs; and
- risks relating to hardware, malicious software and unauthorized actors.

Those minting, selling or purchasing NFTs should be aware of, and understand, these disclosures, and companies building out NFT platforms should carefully consider what disclosures they want to make.

Jurisdiction and applicable law

The foregoing issues are further complicated given that it may not be clear which jurisdiction's laws should apply. One must factor in that NFTs are offered on a decentralized blockchain ecosystem, generally paid for in cryptocurrencies, and can be transferred from one party to another without either party revealing any geographic-identifying information such as a shipping or billing address. Although the terms of use for most NFT marketplaces include a governing law provision, that law would likely only apply to disputes arising between the user and the marketplace itself and would not itself determine the governing law under which to assess rights in the work associated with the NFT. As the use of NFTs and blockchain technology expands, it will likely take a series of court cases, at least in the United States, to establish a framework around how these issues are to be resolved, similar to the jurisdictional case law that developed during the early days of domain name adoption. We may also see NFTs develop such that the metadata specifies the applicable governing law for the NFT and its associated work and that NFT purchases are contingent on acceptance of that law. NFT issuers must also consider that by issuing NFTs that are available for purchase globally, they may be availing themselves of the laws of other jurisdictions and may become subject to additional legal requirements in such jurisdictions.

Anti-money laundering considerations

Since late 2021, the Financial Action Task Force ("FATF") – an intergovernmental organization that develops standards to combat money laundering and terrorism financing – and the U.S. Department of the Treasury ("Treasury")[43] have issued statements regarding the regulatory treatment of NFTs and potential implications for certain NFT market participants under anti-money laundering ("AML") regulatory frameworks. In October 2021, FATF issued updated virtual asset guidance[44] addressing the potential regulatory treatment of NFTs. While FATF is not a regulatory agency, its membership comprises 37 countries, including the United States, and two regional bodies, and it has played an active role in proposing a regulatory framework for virtual assets. In its updated guidance, FATF took the position that "collectible" NFTs will generally not be considered "virtual assets" as defined by FATF,[45] and therefore persons that deal in such NFTs are generally not subject to AML obligations on that basis alone. FATF noted, however, that "it is important to consider the nature of the NFT and its functions in practice and not what terminology or

marketing terms are used." In other words, if used for payment or investment purposes, an NFT could be viewed as a "virtual asset." For this reason and because of the fast pace of development of digital assets, FATF recommended that countries consider the application of FATF standards to NFTs on a case-by-case basis. FATF reaffirmed its guidance on the regulatory treatment of NFTs in a June 2022 update regarding virtual assets.[46]

While FinCEN has not provided specific guidance as to the application of current U.S. AML laws and regulations to NFTs, in February 2022, Treasury discussed NFTs in the context of its Congressionally mandated "Study on the Facilitation of Money Laundering and Terror Finance Through the Trade in Works of Art" (the "Treasury Artwork Study") and offered some insight into broader departmental thinking on NFTs and NFT platforms.[47] Consistent with the FATF Guidance, the Treasury Artwork Study stated that, "[d]epending on the nature and characteristics of the NFTs offered, these platforms may be considered virtual assets service providers (VASPs) by FATF and may come under FinCEN's regulations."[48] In further accord with FATF, the Treasury Artwork Study stated that, while "collectible" NFTs would generally not be treated as FATF-defined "virtual assets," service providers of NFTs or other digital assets that are used as means of payment of investment could meet the FATF definition of VASP.[49] Moreover, Treasury clarified that certain parties involved in the transferring of virtual assets (e.g., virtual currencies) in the course of the purchase or sale of NFTs may be considered money services businesses ("MSBs") under FinCEN's regulations if they are doing business in the United States and have corresponding AML regulatory requirements.[50]

MSBs are required to register with FinCEN and must comply with extensive requirements under the Bank Secrecy Act ("BSA"), including implementing a risk-based AML compliance program, filing suspicious activity reports and maintaining certain records. Foreign-located companies that do business as an MSB wholly or in substantial part within the United States are also required to register with FinCEN and comply with the BSA's requirements. Violation of these obligations can result in substantial civil and criminal penalties.

Risks in art trade

Growing concerns by regulators regarding money laundering and sanctions evasion risks in the art trade could have potential implications for persons that deal in NFTs, to the extent regulators perceive similar financial crime risks in digital art. FinCEN issued guidance in March 2021 emphasizing that financial institutions with existing BSA obligations "should be aware that illicit activity associated with the trade in antiquities and art may involve their institutions." The Office of Foreign Assets Control ("OFAC") similarly issued an advisory in October 2020 highlighting the sanctions risks associated with dealings in high-value artwork involving sanctioned persons. In OFAC's view, the opacity of the art market can make it especially vulnerable to money laundering and sanctions violations.

Although participants in the art trade currently are not subject to the BSA on the basis of their dealings in art, recent legislative developments suggest that this has the potential to change in the coming years. Specifically, as part of the Anti-Money Laundering Act of 2022, Congress commissioned the Treasury Artwork Study, in which the Secretary of the Treasury was required to review how trade in artwork facilitates money laundering and the financing of terrorism. Although the Treasury Artwork Study did not recommend any immediate changes to U.S. AML laws or regulations regarding the treatment of digital art, it noted that NFTs can be used to conduct "self-laundering" where, prior to selling to an unwitting third party, criminals who purchase NFTs with illicit funds may first transact with themselves in an effort to create a transaction record.[51] The study also pointed out that digital art is more

susceptible to money laundering than traditional art, as it can be transferred easily (i.e., no physical transfer is required) and quickly. More recently, in February 2023, FATF echoed similar concerns related to the AML risks related to the trade in NFTs.[52]

Recent AML developments

In the past year, the U.S. Department of Justice, Treasury, and FATF have all cautioned regarding the risks that NFTs can be used to further fraudulent schemes, the proceeds of which may be subject to money laundering.[53] In September 2022, Treasury published an Action Plan to Address Illicit Financing Risks of Digital Assets that called for Treasury to "[p]repare and publish a risk assessment by July 2023 on the money laundering and terrorist financing risks related to NFTs."[54] As of the date of this chapter, Treasury has not published this risk assessment. In the same month, the U.S. Department of Justice released a report supporting "amendments to the BSA and its implementing regulations to make clear that its key AML/CFT provisions—including the obligations to have customer identification programs and report suspicious transactions to regulators—apply to NFT platforms, including online auction houses and digital art galleries."[55] Furthermore, the U.S. government has not taken action to amend the BSA to impose these requirements on NFT platforms, and it is unlikely that such changes will be forthcoming in the coming year.

Securities law considerations

The programmability of NFTs also allows the creator to easily fractionalize ownership of the NFT among multiple parties. One aim of fractional NFTs ("F-NFTs") is to provide a broader group of buyers with the ability to take part in the purchase of rare or expensive digital assets. Although there are a variety of ways of doing this, one involves using a "smart contract" program that issues a pre-set number of fungible cryptocurrency tokens (often called "shards"), which function as fractionalized interests in the underlying NFT. These fungible shards might be made available for purchase or sale on secondary exchanges, including through decentralized platforms.

Under the Supreme Court's *Howey* test, an offering or sale of an asset may constitute an "investment contract" (and thus qualifies as a "security") when it represents a transaction involving (1) an investment of money, (2) in a common enterprise, (3) where profits are reasonably expected to be derived from the managerial or entrepreneurial efforts of others. Over the years, courts (including the Supreme Court) have refined the *Howey* analysis, clarifying that a given offer or sale may fall outside the "investment contract" definition when the underlying asset is acquired primarily for personal use rather than passive investment. Moreover, where the "profits" sought by purchasers are based on their own efforts or market forces of supply and demand, the *Howey* test may not be satisfied.

Applying the *Howey* test to the offer and sale of NFTs that represent rights to digital collectibles and artwork, there are strong grounds to conclude that such transactions would not be considered investment contracts under *Howey*. Because each NFT is a unique, one-of-a-kind digital asset, there is arguably no "common enterprise" involved in the NFT's purchase or sale. Further, many purchasers of NFTs buy them because of their consumptive value – that is, the buyers enjoy owning them in their own right, not because of any potential profit that ownership might bring. And even though some buyers of NFTs may seek to profit based on the possibility that they appreciate in value in the future, like comic books, baseball cards and traditional artwork, such value appreciation is likely to be more closely tied to its rarity and market forces than any ongoing managerial or entrepreneurial efforts of the sellers. Given the fact- and circumstance-specific nature of the *Howey* test, each NFT should be assessed on its own to determine whether the investment contract label might apply to its offer or sale.

Moreover, an analysis of an NFT itself does not necessarily end the inquiry. Most cases applying *Howey* have involved an underlying asset that, in and of itself, is indisputably not a security. Nevertheless, courts have held that the manner in which the underlying asset is promoted to purchasers – including all of the concomitant promises made by the seller – may give rise to an investment contract under *Howey* if they create a reasonable expectation of profits based on the managerial efforts of others. Accordingly, one should look to all of the facts and circumstances surrounding an NFT's offer and sale. This comports with the now-famous speech by former SEC Director William Hinman, who, in the context of opining that the cryptocurrency Ethereum should not be considered a security, emphasized that "the analysis of whether something is a security is not static and does not inhere to the instrument" itself – but rather to the way in which it is offered and sold. That position has been adopted by some courts as well. See, e.g., *SEC v. Ripple*, No. 20 CIV. 10832 (AT), 2023 WL 4507900 (S.D.N.Y. July 13, 2023), and *SEC v. Telegram*, 448 F. Supp. 3d 352 (S.D.N.Y. 2020). Even where an NFT is itself not a security, however, it may be possible for it to be sold as an investment contract under certain facts and circumstances.

One specific circumstance that gives rise to potential securities questions is where NFTs are fractionalized into F-NFTs. As SEC Commissioner Hester Peirce has noted, fractional interests in an NFT may be considered unregistered securities, even if the NFT itself does not qualify as one. As a result, one should consider all of the circumstances of any offer or sale of F-NFTs to assess whether they could be considered an investment contract under *Howey*. This includes assessing the ways in which the F-NFTs are marketed to potential buyers, as well as the promoter's ongoing role with respect to the F-NFTs before and after they are sold.

For example, consideration should be given to the promoter's ongoing role, if any, with respect to the underlying NFT, including any control over future sales of the NFT for profit to benefit all holders of F-NFT shards. On the other hand, where the associated protocol allows F-NFT purchasers to control the NFT through consolidated ownership, and thus to independently determine how to use or sell the NFT to future buyers, this would cut against any argument that the purchasers are relying on the efforts of others to realize a profit. Additionally, where the marketing of the F-NFT places emphasis on the consumptive value of the NFTs or F-NFTs (as opposed to the potential for investment returns based on the promoter's ongoing efforts), there is less risk that they would be deemed investment contracts under *Howey*.

A number of lawsuits have been filed by private plaintiffs alleging that NFTs were offered and sold as unregistered securities, and decisions in those cases may provide further guidance on these issues. See, e.g., *Friel v. Dapper Labs*, No. 21 CIV. 5837 (VM), 2023 WL 2162747 (S.D.N.Y. Feb. 22, 2023), and *Harper v. O'Neal*, No. 23-cv-21912 (S.D. Fla.). For example, on February 22, 2023, Judge Victor Marrero of the U.S. District Court of the Southern District of New York issued a novel decision applying the *Howey* test to the offer and sale of NFTs for the first time. The question before the court was whether the plaintiffs adequately alleged that "Top Shot Moments" NFTs ("Moments") constituted investment contracts and therefore securities. Moments were offered and sold on the Top Shot platform, which was alleged to be owned and operated by Dapper Labs. The plaintiffs claimed that, prior to the launch of Moments, Dapper Labs developed and later exclusively controlled a private blockchain to, among other things, offer support for Moments by hosting the Top Shot platform, record sales transactions that occurred on a secondary marketplace that was part of the Top Shot platform ("Marketplace"), and facilitate the validation of Marketplace transactions.

The defendant moved to dismiss the complaint as a matter of law. The court held that, at the pleading stage and accepting all allegations as true, the plaintiffs had adequately alleged violations of Sections 5 and 12(a)(1) of the Securities Act of 1933 by offering Moments without a registration statement. Essential to the court's reasoning was the allegation (assumed as true for purposes of the motion) that Dapper Labs controlled the Marketplace where Moments could be bought and sold, which was alleged to have "significantly, if not entirely, dictate[d] Moments' use and value." Calling the case a "close call," the court acknowledged that its decision was narrow and based on the specific facts as alleged. The court also emphasized that *Howey* analyses are often circumstance-specific, and each NFT project "must be assessed on a case-by-case basis."

Ultimately, as the Dapper Labs lawsuit and others highlight, securities-related questions involving NFTs may hinge on the specific facts and circumstances surrounding their creation, promotion, offer and sale.

* * *

Endnotes

1. As discussed further below, the digital work associated with an NFT is typically not stored on a blockchain.
2. *See* Crystal Koe, *An Unreleased Recording of Whitney Houston Singing at 17-years-old Has Sold as a $1 Million NFT*, MusicTech, Dec. 16, 2021, https://musictech.com/news/music/an-unreleased-recording-of-whitney-houston-singing-at-17-years-old-has-sold-as-a-1-million-nft; Will Gottsegen, *Snoop Dogg's NFT Mixtape Invites Remixes. Does It Authorize Them?*, CoinTech, Mar. 22, 2022, https://www.coindesk.com/layer2/2022/03/02/snoop-doggs-nft-mixtape-invites-remixes-does-it-authorize-them
3. *See Armin's All-Access*, https://aaa.arminvanbuuren.com
4. Generally, DAOs are blockchain-based entities that operate based on a set of pre-defined rules or protocols governed by smart contracts. DAOs leverage blockchain technology to decentralize the organizational structure of a corporation by providing mechanisms to record interests in a transparent and decentralized manner and to permit certain processes to be automated, such as transferring assets or decision-making capabilities.
5. Importantly, there is not a single "blockchain" the way one might speak of a single internet. Rather, blockchain is a type of technological approach, and not all blockchains can necessarily interact with one another.
6. All updates to Ethereum go through the Ethereum Improvement Proposal ("EIP") process. "ERC" stands for Ethereum Request for Comments, and is a type of EIP focused on standards for Ethereum applications, a category that includes tokens.
7. There are 100 million satoshis in a single Bitcoin.
8. 17 U.S.C. § 106.
9. As a general matter, under U.S. law, copyright vests in the creator of a work with two exceptions: if a work is created by an employee in the course of their employment, copyright vests in the employer, and for certain limited categories of works, if the work is created by an independent contractor under a "work made for hire" agreement, copyright vests in the commissioning party. 17 U.S.C. § 101. In these cases, the employer or the commissioning party enjoys the "bundle of rights" with respect to the work.
10. *See*, *e.g.*, *Rooney v. Columbia Pictures Indus., Inc.*, 538 F. Supp. 211, 223 (S.D.N.Y. 1982), *aff'd*, 714 F.2d 117 (2d Cir. 1982).
11. 17 U.S.C. § 106A.

12. *See*, *e.g.*, 15 U.S.C. § 1114.
13. *See*, *e.g.*, *id.* § 1125.
14. *Rogers v. Grimaldi*, 875 F.2d 994, 999 (2d Cir. 1989).
15. *E.S.S. Ent. 2000, Inc. v. Rock Star Videos, Inc.*, 547 F.3d 1095, 1099 (9th Cir. 2004) (alterations in original) (citation omitted); *see also Rogers*, 875 F.2d at 999.
16. *Hermès Int'l v. Rothschild*, 22-CV-384 (JSR) (S.D.N.Y. Feb. 2, 2022).
17. *Hermès Int'l v. Rothschild*, 22-CV-384 (JSR) (S.D.N.Y. May 18, 2022).
18. *Yuga Labs, Inc. v. Ripps*, CV 22-4355-JFW(JEMX), 2023 WL 3316748, at *12 (C.D. Cal. Apr. 21, 2023).
19. Letter from Thom Tillis, U.S. Senator, and Patrick Leahy, U.S. Senator, to Kathi Duval, Under Secretary of Commerce and Director of the U.S. Patent and Trademark Office, U.S. Patent and Trademark Office, and Shira Perlmutter, Register of Copyrights and Director, U.S Copyright Office (June 9, 2022), https://www.copyright.gov/laws/hearings/response-to-june-9-2022-letter.pdf; Letter from Kathi Duval, Under Secretary of Commerce and Director of the U.S. Patent & Trademark Office, U.S. Patent and Trademark Office, and Shira Perlmutter, Register of Copyrights and Director, U.S Copyright Office to Thom Tillis, U.S. Senator, and Patrick Leahy, U.S. Senator (July 8, 2020), https://www.copyright.gov/laws/hearings/response-to-june-9-2022-letter.pdf
20. The Filecoin protocol that complements IPFS seeks to address this situation by rewarding nodes on the network that maintain redundant copies of files.
21. *Introducing the NFT License*, NFTLicense.org, https://www.nftlicense.org/ (last visited Aug. 16, 2020).
22. *Ownership*, Bored Ape Yacht Club, https://boredapeyachtclub.com/#/terms (last visited Aug. 16, 2020).
23. 17 U.S.C. § 109(a).
24. *Quality King Distribs., Inc. v. L'anza Rsch. Int'l, Inc.*, 523 U.S. 135, 152 (1998).
25. *Capitol Recs., LLC v. ReDigi Inc*., No. 16-2321 (2d Cir. Dec. 12, 2018).
26. 17 U.S.C. § 109; *Apple Inc. v. Psystar Corp.*, 658 F.3d 1150, 1155 (9th Cir. 2011).
27. *Specht v. Netscape Commc'ns Corp.*, 306 F.3d 17, 35 (2d Cir. 2002).
28. *Sgouros v. TransUnion Corp*., No. 14 C 1850, 2015 WL 507584, at *4 (N.D. Ill. Feb. 5, 2015).
29. *Nguyen v. Barnes & Noble, Inc.*, 763 F.3d 1171 (9th Cir. 2014).
30. *Specht* at 19.
31. *Hines v. Overstock.com Inc.*, 380 F. App'x. 22, 2010 U.S. App. LEXIS 11265 (2d Cir. N.Y. 2010).
32. *In re Zappos.com Inc.*, 893 F. Supp. 2d 1058, 2012 WL 4466660 (D. Nev. 2012).
33. *Nguyen* at 1179.
34. *Berman v. Freedom Fin. Network, LLC*, --- F.4th ----, No. 20-16900, 2022 WL 1010531 (9th Cir. Apr. 5, 2022).
35. *Long v. Provide Com., Inc.*, 245 Cal. App. 4th 855, 200 Cal. Rptr. 3d 117 (2d Dist. 2016), and *Sellers v. JustAnswer LLC*, 73 Cal. App. 5th 444, 289 Cal. Rptr. 3d 1 (4th Dist. 2021), *petition for review filed*, No. S273056 (Cal. Feb. 8, 2022).
36. *Berman* at 12.
37. *Berman* at 14.
38. Under Section 512 of the Copyright Act, "provider of online services or network access, or the operator of facilities therefor" are themselves not liable for copyright infringement by third parties using their services where such services are providing "information location tools" (e.g., search functionality). Most NFT marketplaces offer DMCA take-down language to take advantage of this safe harbor.

39. 17 U.S.C. § 512(h).
40. *See*, *e.g.*, *A&M Recs., Inc. v. Napster, Inc.*, 239 F.3d 1004, 1019 (9th Cir. 2001).
41. A plaintiff could analogize today's NFT marketplaces to those of the swap meet operator in *Fonovisa, Inc. v. Cherry Auction, Inc.*, 76 F.3d 259, 264 (9th Cir. 1996). According to the Ninth Circuit, the infringing activity (sales of counterfeits) could not have taken place without all the infrastructure offered by the swap meet provider.
42. *Perfect 10 v. Amazon.com, Inc.*, 508 F.3d 1146, 1171 (9th Cir. 2007).
43. The Financial Crimes Enforcement Network ("FinCEN") is the Treasury Department bureau responsible for administering and enforcing the Bank Secrecy Act ("BSA") – the main AML legislative and regulatory framework applicable to U.S. financial institutions.
44. FATF, "Updated Guidance for a Risk-Based Approach, Virtual Assets and Virtual Asset Service Providers," October 2021. A "virtual asset" is a "digital representation of value that can be digitally traded or transferred and can be used for payment or investment purposes." *FATF Guidance.*
45. FATF Guidance.
46. FATF, "Targeted Update on Implementation of the FATF Standards on Virtual Assets and Virtual Asset Service Providers," June 2022.
47. *See* U.S. Department of the Treasury, "Study of the Facilitation of Money Laundering and Terror Finance Through the Trade in Works of Art," February 2022, https://home.treasury.gov/system/files/136/Treasury_Study_WoA.pdf (hereinafter *Treasury Artwork Study*).
48. Treasury Artwork Study at 26.
49. Treasury Artwork Study at 26.
50. Treasury Artwork Study at 26.
51. Treasury Artwork Study at 27.
52. FATF, "Money Laundering and Terrorist Financing in the Art and Antiquities Market," February 2023, ¶¶ 50–51.
53. *See* U.S. Department of Justice, "The Report of the Attorney General Pursuant to Section 5(b)(iii) of Executive Order 14067: The Role Of Law Enforcement In Detecting, Investigating, And Prosecuting Criminal Activity Related To Digital Assets," September 6, 2022, 11–12, 18; FATF, "Money Laundering and Terrorist Financing in the Art and Antiquities Market," February 2023, ¶¶ 50–51; and U.S. Department of the Treasury, "Illicit Finance Risk Assessment of Decentralized Finance," April 6, 2023, 22–23.
54. U.S. Department of the Treasury, "Action Plan to Address Illicit Financing Risks of Digital Assets," September 16, 2022, 10.
55. U.S. Department of Justice, "The Report of the Attorney General Pursuant to Section 5(b)(iii) of Executive Order 14067: The Role Of Law Enforcement In Detecting, Investigating, And Prosecuting Criminal Activity Related To Digital Assets," September 6, 2022, 42–43.

* * *

Acknowledgments

The authors are grateful for the contributions of Skadden attorneys Mana Ghaemmaghami, Eryn Hughes, MacKinzie Neal, and Jim Perry to this chapter.

Stuart Levi
Tel: +1 212 735 2750 / Email: stuart.levi@skadden.com
Stuart D. Levi is co-head of Skadden's Intellectual Property and Technology Group, and he coordinates the firm's blockchain, outsourcing and privacy practices. Mr. Levi has a broad and diverse practice that includes blockchain and digital asset mattes, technology and intellectual property licensing, fintech matters, privacy and cybersecurity advice, outsourcing transactions, branding and distribution agreements, technology transfers, strategic alliances and joint ventures. Mr. Levi also counsels clients on intellectual property strategy and regulatory compliance.

Eytan Fisch
Tel: +1 202 371 7314 / Email: eytan.fisch@skadden.com
Eytan Fisch advises clients on regulatory and enforcement matters, with a focus on economic sanctions, anti-money laundering, fintech, blockchain and virtual currency matters. He has extensive experience representing global financial institutions and multinational companies on complex cross-border compliance and enforcement matters, including internal investigations, voluntary disclosures, and administrative and enforcement proceedings. Mr. Fisch joined Skadden after nearly six years with the U.S. Department of the Treasury, where he held a variety of senior positions.

Alex Drylewski
Tel: +1 212 735 2129 / Email: alexander.drylewski@skadden.com
Alexander C. Drylewski's practice focuses on high-stakes complex commercial litigation around the world. He represents companies and individuals in high-profile commercial litigation involving emerging technologies, government investigations, securities class actions, trials and appeals.
Mr. Drylewski's representative matters include: advising numerous clients in connection with blockchain/distributed ledger technologies and related litigation and regulatory issues, including with respect to digital tokens, stablecoins and decentralized finance projects; and representing individuals and companies in numerous SEC investigations and enforcement actions relating to the offer and sale of digital assets.

Dan Michael
Tel: +1 212 735 2200 / Email: daniel.michael@skadden.com
Daniel Michael represents entities and individuals, including NFT issuers and trading platforms, in securities-related regulatory investigations and examinations. In addition, Mr. Michael has conducted internal investigations and has advised clients on crisis management, regulatory risk assessments, and on the development and enhancement of policies and procedures designed to prevent and detect potential violations of law.
Prior to joining Skadden, Mr. Michael served as the chief of the SEC Enforcement Division's Complex Financial Instruments Unit, where he oversaw a nationwide team of attorneys and market specialists in investigations and enforcement actions involving complex financial products and market practices.

Skadden, Arps, Slate, Meagher & Flom LLP

One Manhattan West, New York, New York 10001, USA
Tel: +1 212 735 3000 / URL: www.skadden.com

Cryptocurrency compliance and risks: A European KYC/AML perspective

Fedor Poskriakov & Christophe Cavin
Lenz & Staehelin

Introduction

The rapid development, increased functionality, and growing adoption of new technologies and related payment products and services globally continue to pose significant challenges for regulators and private sector institutions in ensuring that virtual currencies and other virtual assets ("**VAs**") are not misused for money laundering ("**ML**") and financing of terrorism ("**FT**") purposes. The underlying reasons for this are numerous and some of such risks were already identified and discussed in 2013 in the Financial Action Task Force ("**FATF**") NPPS Guidance,[1] even though the said report did not specifically refer to "virtual currencies" at the time.

A significant number of VAs have emerged over the years and some VA projects continue to attract significant investments in payment infrastructures built on the relevant software protocols. These payment networks and protocols seek to provide a new method for transmitting value over the internet or through decentralised peer-to-peer ("**P2P**") networks.

As decentralised, convertible cryptography-based VAs and related payment systems are gaining momentum, regulators and financial institutions ("**FIs**") around the world are recognising that VAs and the underlying consensus protocols (1) likely represent the future for payment systems, (2) provide an ever-more powerful new tool for criminals, terrorist financiers and other sanctions-evaders to move and store illicit funds, out of the reach of law enforcement, and, as a result, (3) create unique new challenges in terms of ML/FT risks.[2] Although the global volumes and estimates are relatively low, Chainalysis estimated in 2022 that illicit activity represented 0.24% of cryptocurrency volume, up from 0.12% in 2021, although illicit transaction volume reached its highest level ever at approx. USD 20.6 billion.[3] Most notably, 43% of illicit transaction volume was sanctions related, following the designation of certain individuals and entities with cryptocurrency nexuses by the Office of Foreign Assets Control ("**OFAC**") of the U.S. Department of the Treasury.

Given the trans-jurisdictional (or borderless) nature of the VA phenomenon, major institutions at the international level have all focused on and issued reports addressing VAs and the risks associated with them, including ML/FT risks. FATF and the European Banking Authority (the "**EBA**"), in particular, have issued recommendations in this context, concluding that VA exchange platforms allowing the conversion of VAs into fiat money (and *vice versa*) are of particular relevance and must be brought within the scope of the respective national anti-money laundering and counter-financing of terrorism ("**AML/CFT**") frameworks. In view of the development of additional products and services, as well as the introduction of new types of providers in VA space, FATF adopted changes to its Recommendations in October 2018 to explicitly clarify that they apply to financial activities involving VAs and certain virtual asset service providers ("**VASPs**"). In June 2019, FATF adopted an

Interpretive Note to Recommendation 15 to further clarify how FATF requirements should apply in relation to VAs and VASPs, and issued guidance for a risk-based approach to VAs and VASPs (the "**June 2019 Standards**"). The June 2019 Standards detail the full range of obligations applicable to VASPs as well as to VAs under the FATF Recommendations. In October 2021, FATF released its Updated Guidance for a Risk-Based Approach to Virtual Assets and Virtual Asset Service Providers (the "**Updated Guidance**"), which is an update to the June 2019 Standards. Although not legally binding on FATF member countries, the Updated Guidance forms part of FATF's ongoing monitoring of the VA and VASP sector and constitutes recommendations on how to supervise and regulate VAs and VASPs.

Key potential risks

Key definitions and concepts

(a) *Definitions*

There is no single global definition of the term "crypto- or virtual currency". In 2012, the European Central Bank (the "**ECB**") defined virtual currencies as "*a type of unregulated, digital money, which is issued and usually controlled by its developers, and used and accepted among the members of a specific virtual community*".[4] In 2014, the EBA defined virtual currencies as a "*digital representation of value that is neither issued by a central bank or a public authority, nor necessarily attached to a [fiat currency], but is accepted by natural or legal persons as a means of payment and can be transferred, stored or traded electronically*".[5] In its 2014 report on key definitions of virtual currencies, FATF first gave the following definition: "*[T]he digital representation of value that can be digitally traded and functions as: (i) a medium of exchange; and/or (ii) a unit of account; and/or (iii) a store of value, but does not have legal tender status (i.e., when tendered to a creditor, is a valid and legal offer of payment) in any jurisdiction. It is not issued nor guaranteed by any jurisdiction, and fulfils the above functions only by agreement within the community of users of the virtual currency.*"

In order to provide for a common regulatory approach through the fifth Anti-Money Laundering Directive ("**MLD5**", see also "Current legal and regulatory regime, MLD5", below), the EU decided to adopt a definition of virtual currencies deriving from FATF's 2014 guidance. According to MLD5, a virtual currency is defined as a digital representation of value that is not issued or guaranteed by a central bank or a public authority, is not necessarily attached to a legally established currency, and does not possess a legal status of currency or money, but is accepted by natural or legal persons as a means of exchange, and which can be transferred, stored and traded electronically. Given the broad nature of this definition, it is likely that, in practice, most forms of VAs and other transferable cryptographic coins or tokens (as we know them today) fall within the scope of MLD5.

In parallel, FATF introduced the following definition of VAs in its October 2018 updated Recommendations: "*[D]igital representation of value that can be physically traded, or transferred, and can be used for payment or investment purposes (but do not include digital representations of fiat currencies, securities and other financial assets that are already covered elsewhere in the FATF Recommendations)*."[6]

For the purposes of this chapter, we will adopt the definitions and conceptual framework set out in FATF's Recommendations.[7] In this respect, we will focus on decentralised convertible VAs and related payment products and services ("**VCPPS**"), to the exclusion of other VA-related securities and/or derivatives products and services, even though these are also relevant for ML/FT risk assessment, in particular crowdfunding methods like initial coin offerings ("**ICOs**").

(b) *KYC and transaction monitoring*

Know Your Customer ("**KYC**") is the cornerstone of the AML/CFT due diligence requirements that are generally imposed on FIs whose AML/CFT legislation is aligned with international standards. KYC requirements are relatively recent, as they were first implemented in the 1970s in both Swiss and U.S. legislation, before becoming an internationally recognised concept through the issuance of the FATF Recommendations. KYC requires that FIs duly identify (and verify) their contracting parties (i.e., customers) and the beneficial owners (namely when their contracting parties are not natural persons) of such assets, as well as their origin. Together with transaction monitoring, KYC ensures the traceability of assets, including those remaining in the financial system (i.e., paper trail), and allows the identification of ML/FT indicia.

Although KYC and transaction-monitoring requirements were globally implemented at a time when VAs did not exist, it appears today, based on the various initiatives both at the international and national levels, that the application of AML/CFT requirements to VCPPS remains to be clarified.

One of the challenges is that KYC and other AML/CFT requirements were designed for a centralised intermediated financial system, in which regulatory requirements and sanctions can be imposed in each jurisdiction by competent authorities at the level of FIs operating on its territory (i.e., acting as "gatekeepers"). By contrast, VCPPS rely on a set of decentralised cross-border virtual protocols and infrastructure elements, neither of which typically has a sufficient degree of control over or access to the underlying value (asset) and/or information, so that identifying a touchpoint for implementing and enforcing compliance with AML/CFT requirements is naturally challenging.

Potential ML/FT risks

It has to be recognised that like any money-transmitting or payment services, VCPPS have legitimate uses, with prominent venture capital firms investing in VA start-ups and developing infrastructure platforms. VAs may, for example, facilitate micro-payments, allowing businesses to monetise very low-cost goods or services sold on the internet. VAs may also facilitate international remittances and support financial inclusion in other ways, so that VCPPS may potentially serve the under- and un-banked.

However, most VAs by definition trigger a number of ML/FT risks due to their specific features, including anonymity (or pseudonymity), traceability and decentralisation. Many of those risks and uses materialise not on the distributed ledger ("**DL**") of the relevant VA, but rather in the surrounding ecosystem of issuers, exchangers and users. Rapidly evolving technology and the ease of new cryptocurrency creation are likely to continue to make it difficult for law enforcement and FIs alike to stay abreast of new criminal uses, so that integrating those in a solid KYC/client due diligence ("**CDD**") framework is a never-ending task.

In addition to potential illicit uses of VCPPS, the use of VAs may facilitate ML by relying on the same basic mechanisms as those used with fiat currency, with a significant potential for abuse of unregulated and decentralised borderless networks underpinning VAs. In a nutshell:

- **Placement**: VAs offer the ability to open a significant number of anonymous or pseudonymous wallets, at no or very low cost, something that is a low-risk method of rapidly placing proceeds of illicit activity.
- **Layering**: VAs enable the source of funds to be obfuscated by means of multiple transfers from wallet to wallet and/or their conversion into different types of VAs across borders. This allows for an easy layering without significant cost or risk, it being understood that recent technological developments such as "atomic swaps"

may even further facilitate the misuse of VAs. Incidentally, substantial demand for unregistered ICOs may allow criminals (assuming they control the ICO) to hijack the popular crowdfunding mechanism to convert VA proceeds into other VAs and/or fiat currencies, while adding a seemingly legitimate "front" for the source of funds.

- **Integration**: the use of VAs to acquire goods or services, either directly or through the conversion of the VAs into fiat currency, is facilitated by the ever-increasing list of goods and services for which payment in VAs is accepted, as well as the entry into the VA markets of institutional players both for investment and trading (speculation) purposes, providing substantial liquidity in the VA markets and thereby potentially facilitating large-scale integration by abusing unsuspecting institution actors/investors. Likewise, ICOs with below-average KYC requirements may be abused by criminal actors who may be able to convert their illicit VA holdings into other tokens through subscribing to an ICO, and then exiting the investment immediately upon the relevant coins or tokens becoming listed on any VA exchange.

Naturally, ML/FT risks are heightened among the unregulated actors and service providers in the cryptocurrency markets. Given regulatory pressure to reject anonymity and introduce AML controls wherever cryptocurrency markets interface with the traditional financial services sector, there are new VAs being created to be more compatible with existing regulations.

However, until such time as novel technological solutions are in place, ML/FT risks are typically addressed by imposing strict AML/KYC requirements on "gatekeepers" such as VA exchangers and other FIs. However, according to the Impact Assessment of the European Commission of July 2016,[8] depending on the evolution of the network of acceptance of VAs, there might come a point in time when there will no longer be a need to convert VAs back into fiat currency if VAs become widely accepted and used. This presents a critical challenge in itself, insofar as it will reduce the number of "touchpoints" (i.e., conversion points from VA to fiat, exchangers, etc.) with the traditional intermediated financial services sector and thereby limit the opportunities for ML/FT risk mitigation through regulation of defined intermediaries. The updated FATF Recommendations, however, significantly extended the scope of entities subject to AML/CFT regulation by ensuring that not only VA activities that intersect with and provide gateways to and from the traditional regulated financial system (in particular VA exchangers), but also crypto-to-crypto exchange platforms, ICO issuers, custodial wallets and other related service providers, are regulated for AML/CFT purposes (see "Current international initiatives", below). As new types of VAs and related services such as decentralised finance ("**DeFi**") emerge, the Updated Guidance further extends the scope of entities subject to AML/CFT regulation by clarifying the status of stablecoins, decentralised exchanges, DeFi applications, decentralised or distributed applications ("**DApps**"), VA escrow services, kiosk (or ATMs) providers, as well as entities involved with non-fungible tokens ("**NFTs**"), P2P platforms and self-hosted wallet providers.

Anonymity/pseudonymity

By definition, decentralised systems are particularly vulnerable to anonymity risks. Indeed, in contrast to traditional financial services, VA users' identities are generally unknown, although in most cases they are only pseudonymous, and there is no regulated intermediary that may serve as "gatekeeper" for mitigation of ML/FT risks.

The majority of VAs, such as *Bitcoin* ("***BTC***") or *Ether* ("***ETH***"), have anonymity or pseudonymity by design. The user's identity is not linked to a certain wallet or transaction. However, while a user's identity is not visible on the relevant DL underpinning the VA infrastructure, information on transactions, such as dates, value and the counterparties'

addresses, are publicly recorded and available to anyone. For the purposes of their investigation and prosecution work, enforcement authorities are therefore able to track transactions to a point where the identity may have been linked to an account or address (e.g., wallet providers or exchange platforms).

Some VAs, such as Dash, Monero or Zcash and other "privacy coins", go even further, as they are designed to be completely anonymous: wallet addresses, transactions and information on transactions are not publicly recorded on the relevant DL and provide for complete anonymity, preventing the identification of the legal and beneficial owner of the VAs.

In addition, a number of solutions have emerged that allow a certain enhancement of the anonymity and seek to limit traceability of transactions on otherwise pseudonymous VA networks. For instance, mixing services (also known as "*tumblers*" or "*washers*") aggregate transactions from numerous users and enable the actual paper trail of the transactional activity to be obscured. However, while the precise trail of individual transactions might be obscured, the fact that mixing activity has occurred is detectable on the relevant DL.

Traceability

Although the anonymous or pseudonymous design of VAs is an obvious risk of ML/FT, the public nature of the DL acts as a mitigant by offering a complete transaction trail. The DL is an immutable, auditable electronic record of transactions whose traceability may, however, be limited due to user anonymity and anonymising service providers that obfuscate the transaction chain (see also "Technological solutions?", below).

The traceability or "trail" risks may not be significant when dealing with a single DL or VA protocol. However, the situation becomes much more complex when considering cross-VA exchanges where it may not necessarily be possible to easily trace conversion transactions from one VA/DL to another, given that such tracing may require access to off-chain records of intermediaries or exchangers, which may be unregulated, and located in multiple jurisdictions. Likewise, with the emergence of technological solutions allowing for so-called "atomic swap", or atomic cross-chain trading, traceability will become an even greater challenge. In essence, it will allow users to cross-trade different VAs without relying on centralised parties or exchanges.

Decentralisation

Most VAs are decentralised, i.e., they are distributed on a P2P basis and there is no need for validation by a trusted third party that centrally administers the system. As noted by FATF, law enforcement cannot target one central location or entity (administrator) for investigative or asset-seizure purposes, and customers and transaction records are typically held by different parties, in multiple jurisdictions, making it more difficult for law enforcement and regulators to access them.[9]

This problem is exacerbated by the rapidly evolving nature of the underlying DL technology and VCPPS business models. Without proper safeguards in place, transition from a VCPPS to the fiat financial system may be facilitated by unsuspecting VA exchangers and/or abused by complicit VCPPS infrastructure providers who deliberately seek out jurisdictions with weak AML/CFT regimes or deficient implementation of related controls.

Legal and regulatory challenges

Current legal and regulatory regime

Despite calls for the adoption of global AML standards for VAs, no such uniform rules have yet emerged. However, we have seen some convergence towards the logical FATF view that VCPPS should be subject to the same obligations as their non-VA counterparts. In this

respect, the majority of European jurisdictions that have issued rules or guidance on the matter have typically concluded that the exchange of VA for fiat currency (including the activity of VA "exchanges") is or should be subject to AML obligations.

Differences in national regulations include: (1) varying licensing requirements for VA exchangers, wallet services and other VASPs; (2) treatment of ICOs from an AML regulatory standpoint; and (3) the extent to which crypto-to-crypto exchange is treated differently from crypto-to-fiat exchange. In many cases, the regulatory status of these activities is either ambiguous or case-specific, and partially dependent on new legislation or regulation being adopted.

EU

VAs were first addressed at the EU level when the ECB published its VA report in October 2012. The ECB notably acknowledged that the degree of anonymity afforded by VAs can present ML/FT risks. The ECB further suggested that regulation "would at least reduce the incentive for terrorists, criminals and money launderers to make use of these virtual currency schemes for illegal purposes".[10]

In July 2014, the EBA issued a formal opinion on VAs, indicating in particular that VAs present high risks to the financial integrity of the EU, notably due to potential ML/FT risks. In its January 2019 report,[11] however, the EBA noted that VA-related activity in the EU was regarded as relatively limited and that such activity does not appear to give rise to implications for financial stability.

MLD5 and MLD6

On July 5, 2016, the European Commission presented a legislative proposal to amend MLD4. The proposal was part of the Commission's Action Plan against FT, announced in February 2016. It also responded to the "Panama Papers"[12] revelations of April 2016.

MLD5 was adopted by the European Parliament in plenary on April 19, 2018 and the Council of the European Union adopted it on May 14, 2018. It was formally published in the EU's *Official Journal* on June 19, 2018 and entered into force on July 9, 2018. Member States had until January 10, 2020 to amend their national laws to implement MLD5. To date, most Member States have fully implemented MLD5, although some of those failed to transpose MLD5 completely within the original prescribed deadlines.

Among different objectives, MLD5 expressly aims at tackling FT risks linked to VAs. In this context, VA exchange platforms and custodian wallet providers have been added in the scope of MLD5. In order to allow competent authorities to monitor suspicious transactions involving VAs, while preserving the innovative advances offered by such currencies, the European Commission concluded that it is appropriate to include in the institutions subject to MLD4 ("obliged entities") all gatekeepers that control access to VAs, and in particular, exchange platforms and wallet providers,[13] as recommended by FATF in its guidance (see "Current international initiatives, FATF", below).

(i) *Providers engaged in exchange services*

Interestingly, MLD5 extends EU AML requirements to "providers engaged in exchange services between virtual currencies and fiat currency". As a result, most crypto-to-fiat (or fiat-to-crypto) exchanges are covered by MLD5. However, crypto-to-crypto exchanges do not seem to be expressly covered by MLD5.

Notwithstanding this, it is still possible that certain crypto-to-crypto exchanges may fall within the scope of MLD5 if their activities are conducted by "obliged entities" for other reasons, such as custodian wallet services (see (ii) below). Further, crypto-to-crypto exchanges could still be regulated at Member State level, depending on how

each Member State incorporates MLD5's provisions into its national law, as well as the FATF Recommendations. Similarly, VA ATMs are not covered under MLD5, but some Member States have introduced more stringent rules that cover those activities.

(ii) *Custodian wallet providers*

Custodian wallet providers are defined as entities that provide services to safeguard private cryptographic keys on behalf of customers, to hold, store and transfer VAs. The definition appears to only include wallet providers that maintain control (via a private cryptographic key) over customers' wallets and the assets in it, in contrast to pure software (non-custodial) wallet providers that provide applications or programs running on users' hardware (computer, smartphone, tablet, etc.) to access public information from a DL and access the network (without having access to or control over the user's private keys).

Further, on July 20, 2021, the European Commission presented an ambitious package of legislative proposals to strengthen the EU's AML/CFT rules, including a sixth AML/CFT Directive ("**MLD6**"), the proposal for the creation of a new EU authority to fight ML, and the implementation of FATF's Recommendation 16, otherwise known as the "travel rule", for transfers of VAs. In this respect, on June 30, 2023, Regulation (EU) 2023/1113 on information accompanying the transfers of funds and certain crypto-assets (also referred to as the "**Transfer of Funds Regulation**") entered into force and will apply as from December 30, 2024. The Transfer of Funds Regulation extends the scope to transfers of crypto-assets, whereby all crypto-asset service providers ("**CASPs**", which have a wider scope of services than FATF's VASPs) shall conduct due diligence on their customers and disclose relevant originator and beneficiary data for all crypto transfers without a minimum threshold (going beyond the FATF's Standards). In addition, strict specific requirements apply for VA transfers between CASPs and unhosted wallets (whereas transfers between two unhosted wallets fall outside the scope of the Transfer of Funds Regulation). The introduction of this so-called "travel rule" for VA transaction will ensure financial transparency on exchanges in crypto-assets and will provide the EU with a solid and proportional framework that complies with the most demanding international standards on the exchange of crypto-assets, in particular FATF's Standards, including Recommendations 15 and 16 of the Updated Guidance.

MiCA

Further, on June 30, 2023, Regulation (EU) 2023/1114 of May 31, 2023 on markets in crypto-assets, also known as MiCA, entered into force, with its provisions set to be rolled out in stages over the subsequent 18 months. MiCA provides a robust legal framework for developing VA markets within the EU. Most notably, MiCA applies to all VAs not currently covered under existing financial services legislation, and establishes uniform European rules for issuers of such VAs as well as for CASPs (which have a wider scope of services than FATF's VASPs). In particular, CASPs will require an authorisation in order to operate within the EU, with national authorities required to issue such authorisations within a three-month timeframe and will be subject to strong requirements to protect consumer wallets and become liable where they lose investors' crypto-assets.

To avoid any overlaps with updated AML legislation, MiCA does not duplicate the AML/CFT provisions as set out in the newly updated Transfer of Funds Regulation. However, the European Securities and Markets Authority ("**ESMA**") will be tasked with maintaining a public register of non-compliant VASPs. In particular, CASPs that were already legally providing their services can continue to do so until the earlier of 18 months after entry into force of MiCA or until they obtain authorisation.

MiCA will fully apply as from June 30, 2024 in relation to asset-referenced tokens ("**ARTs**") and electronic money tokens ("**EMTs**"), with the remainder of the provisions to apply 18 months after MiCA's entry into force, i.e., as from December 30, 2024. In particular, on July 12, 2023, ESMA (in close cooperation with the EBA, EIOPA and ECB) published its first consultation package in relation to regulatory technical standards and implementing technical standards under MiCA, focusing on ART authorisations, qualifying holdings, and complaints handling, and invites feedback by September 20, 2023. The next package is to be published in October 2023. The date for the entry into application of those measures is subject to their adoption by the European Commission and approval by the European Parliament and the Council of the European Union.

Switzerland

The Swiss AML legislation does not provide for a definition of VAs, relying upon FATF's definition used in its 2014 report. That being said, since the revision of the Swiss Financial Market Supervisory Authority ("**FINMA**") AML Ordinance in 2015, exchange activities in relation to VAs, such as money transmitting (i.e., money transmission with a conversion of VAs between two parties), are clearly subject to AML rules. Before this revision took place, both FINMA and the Federal Council had already identified,[14] on a risk-based approach, the increased risks associated with VA exchangers and the necessity for them to be subject to AML requirements. As such, Switzerland was a precursor in the implementation of this rule, which has now become standard.

In a nutshell, the purchase and sale of convertible VAs on a commercial basis, and the operation of trading platforms to transfer money or convertible VAs from a platform's users to other users, are subject to Swiss AML rules, including the so-called "travel rule". Before commencing operations, a provider of these kinds of services must become a member of a self-regulatory organisation.

Since the entry in force on August 1, 2021 of revisions to the AML Ordinance as part of the Swiss DLT-specific legislative amendments, certain service providers that assist clients in transferring VAs as part of a business relationship or have power of disposal over VAs of clients are now also in scope of Swiss AML legislation. This in particular may capture some non-custodial wallet providers, depending on their business model and services.

Because convertible VAs can facilitate anonymity and cross-border asset transfers, FINMA considers trading in it to have heightened ML/FT risks, requiring strict CDD, particularly as regards client identification, beneficial ownership and source-of-funds analysis.

In this context, the applicable thresholds for KYC of the client for VA transactions has been lowered to CHF 1,000 with effect as from January 1, 2021, implementing the latest FATF recommendations. The threshold captures any transaction or series of related transactions, and applies on a monthly basis.

The key AML/CFT compliance requirement, which represents a challenge to FIs providing VSPPS because of the very nature of currently existing VAs, is undoubtedly the "travel rule". This rule requires that information about the client and the beneficiary be transmitted with payment orders.[15] Although no system currently exists at either a national or an international level (such as, for example, SWIFT for interbank transfers) for reliably transferring identification data for payment transactions on a DL, there are practical ways for FIs to still comply with this requirement; however, they are comparatively onerous and therefore severely limit the development of VCPPS. Notwithstanding this, there are several industry initiatives that aim at developing a technical solution to reliable and standardised implementation of the "travel rule" requirements, such as OpenVASP or interVASP. Once

some of those standards are vetted by AML regulators, it should be expected that more VCPPS will be offered on the market and that it will become easier to combine the purely decentralised world of VAs and traditional intermediated financial services.

Managing compliance AML/CFT risks

Although there are developments on the regulatory front in terms of strengthening requirements applicable to VCPPS providers, there has been little guidance by regulators to their respective domestic FIs as to how to approach KYC/CDD from an ML/FT risk assessment perspective when dealing with customers exposed to VA and VCPPS risks, other than a recommendation to adopt a prudent, risk-based approach.

In practice, as with any new line of business, type of client or financial transaction, the central AML/CFT compliance questions for FIs will be whether they: (1) understand the relevant risks; (2) can reasonably manage them; and (3) have the knowledge, tools and resources to do so on an ongoing basis (including policies, procedures, training programmes, etc.). FIs that choose to serve the new types of clients in the VA ecosystem should elaborate and put in place specific policies and procedures to ensure that they are able to comply with their AML obligations despite the VA context.

The specifics of each set of requirements will depend on the type of business, client type and jurisdiction, as well as other factors. That being said, the ability of FIs to confirm the identity, jurisdiction and purpose of each customer, as well as the assessment of the source of wealth and funds, is essential to the fulfilment of AML/CFT requirements. VCPPS actors as customers present specific challenges in each of these aspects, so that FIs must ensure that their policies and procedures allow them to perform these core functions with a degree of confidence that is at least equal to that which FIs would require for their traditional financial services.

Given the varying typology of VCPPS service providers, it is virtually impossible to draw up KYC/CDD standards, procedures and checklists that would be applicable universally. It is therefore understandable that regulators have not issued blanket guidance in this space. As the understanding of VCPPS and related AML/CFT risks evolves, it is likely that international standards and recommendations will emerge, and possibly compliance tools that will simplify the implementation thereof by FIs. In this respect, FIs, VCPPS providers, developers, investors, and other actors in the VA space should seek to develop technology-based solutions that will improve compliance and facilitate the integration of VCPPS with the existing financial system.

Possible avenues to address compliance concerns

Current international initiatives

FATF

(a) *Virtual Currencies – Guidance for a risk-based approach (June 2015 Standards)*
In June 2015, FATF issued specific guidance on virtual currencies, focusing on the points of intersection that provide gateways to the regulated financial system – *Guidance for a Risk-Based Approach: Virtual Currencies* (the "**Guidance**"). This Guidance derives from previous reports of FATF, namely the June 2014 *Virtual Currencies Report* and the FATF NPPS Guidance of June 2013.
In accordance with the cardinal risk-based approach principle, the Guidance provides for a certain number of clarifications on the application of the FATF Recommendations to entities involved in VCPPS.

FATF is of the view that domestic entities providing convertible VA exchange services between VA and fiat currency should be subject to adequate AML/CFT regulation in their jurisdiction, like any other FI, and be subject to prudential supervision. In this context, the distinction between centralised and decentralised VAs is a key aspect for the purposes of the risk assessment to be performed. FATF recommends that entities involved in convertible and decentralised VCPPS be subject to an enhanced due diligence process, as such activities are regarded as higher risk due to the inherent anonymity element and challenges to perform proper identification (i.e., the underlying protocols on which the major part of the decentralised VCPPS are currently based do not provide for the participants' identification and verification) (see also "Anonymity/pseudonymity", above).

It is important to note that FATF does not recommend prohibiting VCPPS. On the contrary, such prohibition could drive such activities underground and lead to a complete lack of visibility and control over them. As a result, in case of prohibition of VCPPS, FATF recommends implementing additional mitigation measures, also taking into account the cross-border element in their activities.

As regards transaction monitoring, FATF is of the view that countries must ensure that originator and beneficial owner information is always included when convertible VA exchangers conduct convertible VA transfers in the form of wire transfers. Certain *de minimis* thresholds may, however, be implemented in order to exclude lower risk transactions. Transaction monitoring remains a key risk mitigant in the convertible VA world, as long as a conversion of VAs occurs.

(b) *FATF Recommendations*

FATF updated its Recommendations in October 2018 to address the rapidly evolving risks related to VAs and to clarify how the FATF Recommendations apply in the case of financial activities involving VAs. The updated Recommendations specifically address and target VASPs, defined as any natural or legal person who is not covered elsewhere under the Recommendations, and as a business conducts one or more of the following activities or operations for or on behalf of another natural or legal person: (i) exchange between VAs and fiat currencies; (ii) exchange between one or more forms of VAs; (iii) transfer of VAs; (iv) safekeeping and/or administration of VAs or instruments enabling control over VAs; and (v) participation in and provision of financial services related to an issuer's offer and/or sale of a VA.

These new definitions significantly expand the scope of entities subject to AML/CFT regulation since the June 2015 Guidance by ensuring that VASPs (not only fiat-to-VA exchanges but also crypto-to-crypto exchange platforms, ICO issuers, custodial wallets and other related service providers) are regulated for AML/CFT purposes, as well as licensed or registered and subject to effective systems for monitoring and ensuring compliance with the relevant measures called for in the FATF Recommendations. That being said, the above-mentioned definitions remain somewhat vague, and their interpretations remain to be determined.

(c) *Interpretive Note to Recommendation 15*

FATF adopted an Interpretive Note to Recommendation 15 on June 21, 2019, setting out requirements for effective regulation, supervision and monitoring of VASPs. Under this note, VASPs should be licensed or registered and be subject to effective regulation and supervision to ensure that they take the necessary steps to mitigate AML/CFT risks. To this end, VASPs should (1) be supervised or monitored by a competent authority (not a self-regulatory body), which should conduct risk-based supervision or

monitoring and have power to impose a range of disciplinary and financial sanctions, and (2) adopt a number of preventive measures to mitigate ML and FT risks (including, but not limited to, CDD, record-keeping, suspicious transaction reporting and screening all transactions for compliance with targeted financial sanctions). In particular, VASPs should conduct CDD for occasional transactions above a USD/EUR 1,000 threshold. According to Paragraph 7(b) of the Interpretive Note, VASPs should obtain and hold required and accurate originator and beneficiary information in relation to VA transfers, and share this information with beneficiary VASPs and counterparts, as well as competent authorities (i.e., the "travel rule"). Further, the specific requirements relating to wire transfers (such as monitoring the availability of information, taking freezing actions and prohibiting transactions with designated persons and entities) as set out under Recommendation 16 would apply on the same basis to transfers of VAs. The Interpretative Note finally highlights the need for international cooperation and information exchange to prevent and combat ML/FT risks associated with VAs.

While the "travel rule" has been a longstanding requirement for FIs internationally, the implementation of this requirement for VASPs to collect and transfer customer information during transactions will undoubtedly present a challenge considering the very nature of DL technologies. Indeed, whereas FIs rely on established interbank communication systems (such as SWIFT, TARGET or SIC) to move funds and share information, no established communication system yet exists for VASPs, and DL technologies – as they stand – usually only require a recipient address to effect a transfer, which renders difficult – if not impossible – ownership verification by VASPs and determination of whether the recipient address is managed by another obliged VASP or a non-custodial wallet that would fall outside the FATF Recommendations.

(d) *Guidance for a Risk-Based Approach to Virtual Assets and Virtual Asset Service Providers (June 2019 Standards)*

In June 2019, FATF published the *Guidance for a Risk-Based Approach to Virtual Assets and Virtual Asset Service Providers*, which builds upon FATF's June 2015 Standards on the risk-based approach to VAs and VASPs and is intended to help both national authorities in understanding and developing regulatory and supervisory responses to VA activities and VASPs, as well as to help VASPs in understanding their AML/CFT obligations. Under the risk-based approach and in accordance with Paragraph 2 of the Interpretative Note, countries should identify, assess, and understand the ML/FT risks in relation to VA financial activities or operations and VASPs and focus their AML/CFT efforts on potentially higher-risk VAs. Similarly, countries should require VASPs to identify, assess, and understand the ML/FT risks. Finally, in a report dated June 2020, FATF confirmed that the June 2019 Standards also apply to stablecoins, as they are to be considered either VAs or traditional financial assets depending on their exact nature. In particular, entities involved in any stablecoins might have AML/CFT obligations, depending on the activities these entities undertake (i.e., an activity of an FI or that of a VASP) and the design of the stablecoin (a key element being the extent to which the stablecoin arrangement is centralised or decentralised). More recently, FATF updated the June 2019 Standards (the Updated Guidance).[16] The Updated Guidance concerns six main areas, namely (i) expanding the definitions for what constitutes VASPS and VAs, (ii) how FATF Standards apply to stablecoins, (iii) additional guidance about risk and risk mitigation for P2P transactions, (iv) updated guidance about the licensing and registration of VASPs, (v) additional guidance about the "travel rule", and (vi) fostering information sharing and cooperation between VASP supervisors (i.e., regulators).

In particular, the Updated Guidance was updated to state that the definitions of VA and VASP are to be interpreted and read "broadly" and that jurisdictions should not determine whether an entity is a VASP based on the technology it uses or the label that the entity applies to itself. The Updated Guidance provides an extensive explanation of the five activities that establish an entity as a VASP, including making it clear that some actors in the VA sector previously thought not to be VASPs are within the definition of a VASP. As a result of this now expanded definition of a VASP, the Updated Guidance states that the creators, owners, operators or some other person who maintains control or sufficient influence of DeFi arrangements are likely VASPs because they provide or actively facilitate VASP services, "even if this is exercised through a smart contract or in some cases voting protocols". In addition, the Updated Guidance also provides that the following entities may also fall within the definition of a VASP: (i) VA escrow services; (ii) brokerage services that facilitate the issuance and trading of VAs; (iii) order-book exchange services; (iv) advanced trading services; (v) VA exchanges or VA transfer services; and (vi) kiosk providers.

In its June 2020 report on stablecoins, as well as in the Updated Guidance, FATF further concluded that stablecoins could either be classified as VAs or traditional financial assets under the revised FATF Standards.[17] In addition, the Updated Guidance states that entities involved in stablecoin arrangements may have AML/CFT obligations either as VASPs or FIs, such as the central developer or governance body who may establish the rules governing the stablecoin arrangement, manage the stabilisation function or the integration of the stablecoin into telecommunication platforms.

The Updated Guidance also affirms that P2P transactions are not subject to FATF AML/CFT obligations because FATF generally places obligations "on intermediaries rather than on individuals themselves". As such, FATF considers that P2P transactions could pose heightened ML or FT risks, especially if they became more widespread and mainstream, so that the Updated Guidance offers measures that jurisdictions could undertake, including measures to increase transparency into P2P transactions, limit the availability of certain P2P transactions, and enhance communication with the private sector to assess and understand the risk of P2P transactions.

Finally, FATF observes that the application of the "travel rule" would be expended insofar as more entities would be considered VASPs under the definitions of VA and VASP as developed in its Updated Guidance, but that jurisdictions may set up a *de minimis* threshold under which AML/CFT obligations would be imposed. Further, sanctions screening and certain due diligence measures have also been introduced on VA transactions.

(e) *Implementation monitoring of the June 2019 Standards*

FATF completed in early July 2020 a review of the implementation of its June 2019 Standards on VAs and VASPs. FATF found that both the public and private sectors have generally made progress in implementing the revised FATF Standards. FATF was advised that 35 out of 54 reporting jurisdictions have implemented the June 2019 Standards, with 32 of these regulating VASPs and three of these prohibiting the operation of VASPs, while the other 19 jurisdictions have not yet implemented the revised Standards into their national law. FATF further noted some progress in the supervision of VASPs and the implementation of AML/CFT obligations by VASPs (although generally still nascent). Progress in the development of technological solutions to enable the implementation of the "travel rule" was noted, although issues remain to be addressed by the public and private sectors for a practical implementation of the recommendations.

In its second 12-month review of the implementation of its revised Standards on VAs and VASPs published on July 5, 2021, FATF found that many jurisdictions have continued to make progress in implementing the revised FATF Standards: 58 out of 128 jurisdictions advised that they have now implemented the revised FATF Standards, with 52 of these regulating VASPs and six jurisdictions prohibiting the operation of VASPs, while the other 70 jurisdictions have not yet implemented the revised Standards into their national law. FATF also noted that only 35 of these 58 jurisdictions that reported having implemented or prohibiting VASPs were currently operational. FATF further observed that the gaps in implementation mean that there is not yet a global regime to prevent the misuse of VAs and VASPs for ML or FT and that the situation allows for jurisdictional arbitrage.

Considering that the VA sector is fast-moving and technologically dynamic, this second 12-month review report recommends that FATF undertakes the following actions: (i) focus on the implementation of the current FATF Standards across its global network; (ii) accelerate the implementation of the "travel rule" by the private sector as a priority, by legal implementation into domestic legislation; and (iii) monitor the VA and VASP industry for any material changes or developments that necessitate further revision or clarification of the FATF Standards considering the fast-changing business and technological environment of VAs.

(f) *Targeted Update on Implementation of FATF Standards on VA and VASPs*

On June 30, 2022, FATF produced a targeted update on the implementation of the FATF Standards, with a focus on FATF's travel rule (the "**Targeted Update**"). The Targeted Update also provides a brief update on the general implementation of FATF's Recommendation 15 and its Interpretative Note, as well as emerging risks and market developments that FATF continues to monitor, such as DeFi, NFTs and unhosted wallets. The Targeted Update builds on the previous 12-month reviews conducted in 2020 and 2021 and finds that many jurisdictions are yet to implement the FATF's travel rule: only 29 countries have currently implemented travel rule requirements applicable to VAs and VASPs and only 11 have started enforcement, out of 98 countries surveyed in March 2022.

The Targeted Update confirms that there are technological solutions to support compliance with the travel rule and providers have started taking steps in ensuring interoperability with other solutions, but encourages further innovations from the private sector to develop operable technological tools enabling global implementation. As regards DeFi, the Targeted Update states that FATF continues to focus on the substance of a transaction rather than terminology and notes that FATF's recent outreach with industry suggests that "decentralised" can currently be a marketing term rather than a technological description, and that even in so-called "decentralised arrangements", there often continues to be persons and centralised aspects that may be subject to AML/CFT obligations. With respect to NFTs, the Targeted Update reiterates the view from the Updated Guidance that NFTs are generally not VAs, but that the FATF Standards should apply in cases where they perform the same function as VAs. FATF will continue to monitor developments and trends, including in respect to DeFi, stablecoins and NFTs.

Further, FATF pushed a report titled "Outcomes FATF Plenary, 21–23 June 2023" outlining the progress – or lack thereof – on its global AML/CFT efforts over the past year.[18] FATF concluded that its AML/CFT rules and recommendations related to VAs and VASPs were largely not being followed, noting that many jurisdictions have not yet implemented fundamental requirements and that more than half of the survey

respondents have not taken any steps towards implementing the travel rule. On June 27, 2023, FATF published another trade update on the implementation of the FATF Standards, with a focus on country compliance with FATF's travel rule, and updates on emerging risks and market developments, including DeFi, P2P transactions and NFTs, unhosted wallets and stablecoins.[19] In particular, FATF reiterated in the Targeted Update its concern over the lack of implementation of FATF's requirements, noting that 75% of jurisdictions are not compliant, or only partially compliant, with such requirements, and that jurisdictions have made insufficient progress on implementing the travel rule, leaving VAs and VASPs vulnerable to misuse.

Latest discussions and developments

Bank for International Settlements

In its statement on VAs of March 2019, the Bank for International Settlements (the "**BIS**") recalled that VAs have exhibited a high degree of volatility and are considered an immature asset class given the lack of standardisation and constant evolution. In this respect, BIS highlighted the various risks that VAs present for banks, including AML/CFT risks, but also liquidity, credit, market, operational, legal and reputation risks. Accordingly, the Basel Committee set out its prudential expectations related to banks' exposures to VAs and related services that banks must, at a minimum, adopt (such as conducting comprehensive analyses of the risks noted above, implementing a clear and robust risk management framework that is appropriate for the risks of VA exposures and related services). According to BIS Paper No. 107 dated January 2020, however, no central bank reported any significant or wide public use of VAs for either domestic or cross-border payments, and the usage of VAs was considered either minimal or concentrated in niche groups.

Further, in its Annual Economic Report dated June 21, 2022, BIS notes a burst of creative innovation in money and payment systems, but concludes that VAs' "structural flaws" make it unsuitable as the basis for a monetary system as VAs lack a stable nominal anchor, while limits to its scalability result in fragmentation, accompanied by congestion and high fees. In particular, BIS notes that even if stablecoins were to remain stable to some extent, they lack the qualities necessary to underpin the future monetary system as they must import their credibility from sovereign fiat currencies, but do not benefit from the regulatory requirements and protections of bank deposits and e-money. From BIS' perspective, there is more promise in sounder representations of central bank money and liabilities of regulated issuers. Indeed, in its Annual Economic Report, BIS reveals a vision for the future of money using central bank digital currencies ("**CBDCs**") to "meld new technological capabilities" with a superior representation of central bank money at its core, at both the wholesale and retail level.

Creation of specific Financial Intelligence Units

The creation of specific Financial Intelligence Units ("**FIUs**") for VA-related transactions could be one of the measures to be implemented at national level that would have an impact at international level. The cooperation between such specific FIUs would improve investigatory assistance and international cooperation in this respect (as stated in the FATF Guidance).

Central bank cryptocurrencies

Based on the various statements and reports on VAs issued by central banks in different jurisdictions, it appears that central banks agree that VAs such as *BTC* and *ETH* are not meant to replace fiat currency. According to the *International Monetary Fund Global Financial Stability Report* dated April 2018, the use of cryptocurrencies as a medium of exchange has been limited and their high volatility has prevented them from becoming a

reliable unit of account. In this context, VAs do not appear to pose macro-critical financial stability risks at present, although if widely used, they may raise issues about, *inter alia*, ML and investor and consumer protection.

Notwithstanding the above, some 80% of central banks (such as Banque de France, Norges Bank and the Bank of England) are currently following the evolution of the developments of VAs and CBDCs closely or even contemplating issuing their own CBDC in order to take advantage of the dematerialisation of the currency (triggering costs reductions) and to facilitate international transactions by avoiding currency exchange issues and providing for instantaneous transfers, security and monitoring capabilities according to BIS Paper No. 107 dated January 2020. In particular, the ECB published in October 2020 a comprehensive report on the possible issuance of a digital euro to complement the current offering of cash and wholesale central bank deposits. The Governing Council of the ECB decided in July 2021 to launch the investigation phase of such digital euro project.

CBDCs could be viewed as a solution to mitigate ML/FT risks, as the transactions related thereto would necessarily go through a regulated financial intermediary subject to AML/CFT regulations. This presupposes a new generation of centralised cryptocurrencies, which will not have the same level of anonymity and transferability as the current cryptocurrencies. In this respect, it is worth noting that BIS indicated in its March 2018 report, *Central bank digital currencies*, that the issuance of CBDCs could come, in addition to more efficient and safer payments and settlement systems, with some benefits from an AML/CFT perspective. To the extent that CBDCs allow for digital records and traces, it could indeed improve the application of rules aimed at AML/CFT, as well as reduce costs of compliance. To date, the Bahamas became the first to launch a general purpose CBDC, known as the Sand Dollar, and several jurisdictions have announced trials and experiments in this respect, such as China, India, Switzerland, and France.

In this context, in some part as a reaction to Facebook's Libra project and also in response to China's plans in the field of digital currencies and payments, a growing demand is forming for some form of programmable digital money that can be integrated into the existing financial system. Indeed, the potential of technology is self-evident – a national currency that is fully programmable becomes *de facto* resilient to ML/FT risks by design and would discourage non-compliant uses of such currency. However, the various risks and legitimate privacy concerns need to be addressed before such a means of payment becomes socially acceptable or desirable.

Technological solutions?

According to certain authors and actors active in the cryptocurrency field, the specific features of DL technologies and protocols could be used to mitigate the ML/FT risks in relation to VAs. KYC, beneficial owner and transactional information could be registered and verified on a dedicated DL, in the form of a global network of unalterable information (or global data repository) that would be accessible by "gatekeepers" and law enforcement. This solution, although very promising at first sight, would raise significant technical and legal issues. Among the latter, one should mention the legal requirements in terms of data protection and, as the case may be, banking secrecy. Furthermore, the access to information and its use by public authorities, such as criminal prosecution authorities, would have to be strictly regulated in order to avoid any intervention outside the applicable mutual assistance channels. In this respect, and as one of the main challenges, such a private DL would need to comply with rules enacted at an international level by the jurisdictions whose FIs

would be involved in such network. It appears, therefore, that there are a certain number of obstacles as of today to using DL technologies for AML/CFT purposes, especially in the absence, at this stage, of clear guidance and standards at international level.

As mentioned in the FATF 2015 report on VAs, other technical solutions may be available. Third-party digital identity systems, as well as new business models, could be developed to facilitate customer identification/verification, transaction monitoring and other due diligence requirements. In particular, in FATF's view, application programming interfaces that provide customer identification information, or allow FIs to set conditions that must be satisfied before a VA transaction can be sent to the recipient, could be used to reduce the ML/FT risks associated with a VCPPS. In its latest targeted update dated June 2023, FATF noted that the private sector now offers a range of technological tools to enable VASPs to implement the travel rule but that these tools generally do not fully comply with all FATF requirements, and recommended that the private sector address any shortcomings rapidly, but also improve the interoperability of travel rule compliance tools globally, whether through technological advancements that allow interoperability between tools or by developing relationships that permit transactions to be made through a chain of interoperable tools. A certain number of fintech companies have already started to develop technological AML solutions.

Conclusion

VCPPS continue to gain momentum. As adoption increases and innovation relevant to AML/CFT compliance becomes embedded in the VCPPS "genetics", we may witness the emergence of improved existing VA protocols or entirely new VAs, built on fundamentally different underlying principles that could include built-in controls, full decentralisation trusted "gatekeepers", digital identity interfaces and transaction monitoring.

Unfortunately, for as long as consistent and recognised standards and/or compliance tools are lacking, many legitimate actors in the VCPPS space will continue to be denied access to traditional banking services in a number of jurisdictions, and/or be "de-risked" by FIs. To the extent that international standard-setters, national regulators, FIs and VCPPS service providers and innovators recognise the opportunities and benefits of VCPPS globally, they should cooperate to define best practices and open, interoperable standards (as opposed to proprietary solutions), as well as training programmes for the next generation of VA "compliance officers". Indeed, applying existing concepts and approaches tailored to an intermediated, centralised financial infrastructure simply does not work when transposed to VA ecosystems, which abide by different rules and principles by design.

* * *

Endnotes

1. *Guidance for a Risk-Based Approach to Prepaid Cards, Mobile Payments and Internet-Based Payment Services*, June 2013, https://www.fatf-gafi.org/media/fatf/documents/recommendations/Guidance-RBA-NPPS.pdf
2. Communication from the Commission of the European Parliament and of the Council on an Action Plan for strengthening the fight against FT, Strasbourg, February 2, 2016.
3. Chainalysis, *The 2023 Crypto Crime Report, Everything you need to know about cryptocurrency-based crime*, February 2023, https://go.chainalysis.com/rs/503-FAP-074/images/Crypto_Crime_Report_2023.pdf

4. European Central Bank, *Virtual Currency Schemes*, October 2012.
5. European Banking Authority, *Opinion on virtual currencies*, July 4, 2014.
6. *Guidance for a Risk-Based Approach to Virtual Assets and Virtual Asset Service Providers*, June 2019, https://www.fatf-gafi.org/media/fatf/documents/recommendations/RBA-VA-VASPs.pdf
7. Available here: https://www.fatf-gafi.org/media/fatf/documents/reports/Virtual-currency-key-definitions-and-potential-aml-cft-risks.pdf
8. Impact Assessment accompanying the document Proposal for a Directive of the European Parliament and of the Council amending Directive (EU) 2015/849 on the prevention of the use of the financial system for the purposes of ML or FT and amending Directive 2009/101/EC, July 5, 2016 ("**MLD4**").
9. FATF, *Virtual Currencies: Key Definitions and Potential AML/CFT Risks*, June 2014.
10. Report of the ECB on Virtual Currency Schemes, October 2012.
11. European Banking Authority, *Report with advice for the European Commission on Crypto-assets*, January 9, 2019, https://eba.europa.eu/sites/default/documents/files/documents/10180/2545547/67493daa-85a8-4429-aa91-e9a5ed880684/EBA%20Report%20on%20crypto%20assets.pdf
12. The documents, some dating back to the 1970s, were created by, and taken from, Panamanian law firm and corporate service provider Mossack Fonseca, and were leaked by an anonymous source.
13. European Commission, *Explanatory Memorandum*, Proposal for a Directive of the European Parliament and of the Council amending MLD4.
14. Swiss Federal Council Report on Virtual Currencies, June 25, 2014.
15. FINMA Guidance 02/2019 – Payments on the blockchain, August 26, 2019.
16. Available here: https://www.fatf-gafi.org/media/fatf/documents/recommendations/Updated-Guidance-VA-VASP.pdf
17. FATF, *Report to the G20 Finance Ministers and Central Bank Governors on So-called Stablecoins*, June 2020, https://www.fatf-gafi.org/media/fatf/documents/recommendations/Virtual-Assets-FATF-Report-G20-So-Called-Stablecoins.pdf
18. FATF, *Outcomes FATF Plenary, 21–23 June 2023*, June 2023, https://www.fatf-gafi.org/en/publications/Fatfgeneral/outcomes-fatf-plenary-june-2023.html
19. FATF, Targeted Update on Implementation of the FATF Standards on Virtual Assets and Virtual Asset Service Providers, June 2023, https://www.fatf-gafi.org/content/dam/fatf-gafi/guidance/June2023-Targeted-Update-VA-VASP.pdf.coredownload.inline.pdf

* * *

Acknowledgment

The authors thank Maria Chiriaeva for her contribution to prior editions of this chapter.

Fedor Poskriakov
Tel: +41 58 450 7131 / Email: fedor.poskriakov@lenzstaehelin.com
Fedor Poskriakov is a partner at Lenz & Staehelin in the Banking and Regulatory group in Geneva and specialises in banking, securities and finance law. He regularly advises on various regulatory, contractual and corporate matters. His practice covers banking, investment management and alternative investments, including private equity and hedge funds. He also heads the firm's Geneva office fintech practice. Highlighted as a "Next Generation Lawyer" (*The Legal 500*, 2019), Fedor Poskriakov is recognised for his "masterful ability to navigate through complex technological aspects of FinTech projects" (*Who's Who Legal*, 2019) and "his great understanding of the blockchain technology itself, combined with his concrete experience in translating this into practice" (*Chambers*, 2019).

Christophe Cavin
Tel: +41 58 450 7000 / Email: christophe.cavin@lenzstaehelin.com
Christophe Cavin is a senior associate in the Geneva office and is a member of the Banking and Finance group and the Investigations group, respectively. His main areas of practice include banking and finance, regulatory, investigations, corporate, commercial and contractual matters. Christophe Cavin is admitted to the Bar in Geneva and New York. He has a Master's in commercial law from the University of Geneva and an LL.M. from the University of Pennsylvania Carey Law School.

Lenz & Staehelin

Route de Chêne 30, CH-1211 Geneva 6 / Brandschenkenstrasse 24, CH-8027 Zurich, Switzerland
Tel: +41 58 450 7000 / +41 58 450 8000 / Fax: +41 58 450 7001 / +41 58 450 8001 / URL: www.lenzstaehelin.com

The regulation of stablecoins in the United States

Douglas Landy, Leel Sinai, Stephen Hogan-Mitchell & Chanté Eliaszadeh
White & Case LLP

Stablecoins are cryptocurrencies that attempt to tie or "peg" their market price to another asset, typically fiat currencies such as the US dollar. Crypto enthusiasts have long viewed stablecoins as a means of bridging the divide between more volatile cryptocurrencies and the traditional financial system. Recently, however, stablecoins have been targeted with increasing legislative and regulatory scrutiny based on their perceived risk to consumers and the financial system. Indeed, there are numerous examples of "runs on the bank," lawsuits and even insolvencies among stablecoin issuers. This chapter will discuss the history and characteristics of certain representative stablecoins, provide a high-level overview of the developing legislative and regulatory environment, discuss the implications of a regulatory framework for stablecoin issuers, and argue that bank-issued stablecoins should be regulated as a banking product – not securities – subject solely to regulation by the prudential bank regulators.

Introduction

The regulatory landscape for stablecoins is marked with uncertainty, particularly at the federal level. Despite this, stablecoins as a technology have achieved significant success, particularly as payment instruments. At the same time, there have been recent examples of spectacular failures of stablecoin issuers and stablecoins, highlighting the need for thoughtful and comprehensive regulation in this space. Our position is that stablecoins should be regulated by issuer, with non-bank issuers being regulated as issuing commodities or securities, and bank issuers being regulated as issuing a banking product akin to a tokenized deposit.

This chapter will begin with an overview of the various kinds of stablecoins as well as their benefits and risks. The second section will survey the current landscape of stablecoin regulation as well as the early successes and more recent failures of these products. The third section will look at past regulatory guidance regarding stablecoins as well as what the future may hold for stablecoin regulation, which will include a deeper dive into one example from New York of what a comprehensive regulatory regime for stablecoins may look like before we conclude in the final section.

What is a stablecoin?

As the term suggests, "stablecoin" refers to a cryptocurrency that attempts to achieve stability relative to an external asset class. Stablecoins attempt to maintain a consistent exchange rate (or "peg") against another asset through a variety of mechanisms that usually, but not always, involve "collateralization" in the form of the issuer holding reserve assets in support of the peg. Stablecoins' relative lack of price volatility and intuitive exchange rate with traditional assets, such as the US dollar (the most popular form of stablecoin by

market capitalization),[1] have made them exceptionally popular as an interface between the traditional and cryptocurrency markets. Indeed, "[t]he stablecoin market is expected to grow to $2.8 trillion in the next five years from $125 billion now."[2]

How do stablecoins work?

A plethora of stablecoin variants have developed since they first emerged in 2014.[3] In general, these stablecoins can be categorized as either "collateralized" or "algorithmic." The former is by far the most popular, while the latter has been responsible for a recent, spectacular market collapse, as discussed below in "Stablecoins in action: early successes and recent failures."

Collateralized stablecoins

Collateralized stablecoins attempt to achieve stability by backing each issued token with a pool of reserve assets, typically (but not always) at a 1:1 reserve ratio.[4] The most common reserve asset is fiat money (money made legal tender by a government fiat or decree). For example, USD Coin ("USDC"), the second-largest stablecoin by market capitalization at the time of writing,[5] purports to back each USDC token with one US dollar (held either in "cash deposits at insured banks or short-dated U.S. treasuries"). Circle, the company responsible for issuing USDC, publishes audit reports and other assurances of this reserve in an effort to increase trust in this collateralization.[6]

Stablecoins need not be collateralized by fiat money, however. Some stablecoins are collateralized with other valuable assets, including commodities (such as gold),[7] bonds and notes, and "baskets" of several different types of assets.[8] Stablecoins may even be collateralized by other cryptocurrencies (so-called "on-chain collateralization").

Algorithmic stablecoins

Instead of (or in addition to) attempting to peg their value to that of an external asset, algorithmic stablecoins attempt to achieve stability by using various autonomous mechanisms to manipulate the supply of the stablecoin in response to fluctuations in the stablecoin's value. These mechanisms can range from the simple "rebase" algorithmic stablecoin – which leverages smart contracts (self-executing computer code) to "burn" (destroy) or "mint" (create) coins when the price deviates from an external peg (e.g., the US dollar) – to the elaborate "seigniorage" algorithms – which use free market behavior models and incentives to manipulate demand for the coin (in addition to supply).

Algorithmic stablecoins attempt to achieve the same benefits of collateralized stablecoins without the expense and operational complexity of a pool of reserve collateral. Unfortunately, they also have unique vulnerabilities. The complexities of their algorithms make them vulnerable to confusion and/or attack; indeed, there have been several recent examples of major algorithmic stablecoins "de-pegging," or losing their fix to the US dollar, and thereby erasing billions of US dollars of value.

What are the benefits and risks of stablecoins?

The primary value-add of stablecoins comes from their relative lack of volatility. In the nascent cryptocurrency market, recent swings have sent the value of the major cryptocurrencies, such as Bitcoin and Ethereum, through exponential booms and busts. In theory, stablecoins offer a safe haven for users who want to avoid this risk while still maintaining assets and transacting in the digital economy. Indeed, their relative stability makes them particularly attractive candidates to integrate the traditional financial system with blockchain-based cryptocurrencies. In contrast to the traditional financial system, stablecoins allow for payments that settle almost instantaneously and often without an intermediary. They can

be sent to "smart contracts," software contracts that can autonomously perform functions that were traditionally relegated to banks, such as escrow reserves, collateralized lending, derivatives, and asset management. Finally, their digital nature makes them well suited to future digital innovations, such as Web3 – a movement to reorganize the internet around decentralized technologies and replace traditional, server-based websites with blockchain-based applications[9] – and the tokenization of financial markets.

At the same time, the current iteration of stablecoins has proven itself to be a significant source of risk to financial stability. Stablecoins have exhibited a pattern of being hacked,[10] losing investor confidence, underselling operational issues or counterparty credit risk, or otherwise "de-pegging" and tumbling in value.[11] These failures have prompted regulators to seriously consider the systemic risks posed by stablecoins and their rapid growth adjacent to the traditional financial ecosystem, and to propose safeguards to ensure that these new technologies do not disrupt financial markets.

How are stablecoins currently regulated in the United States?

Currently, there is no comprehensive, nationwide regulatory framework for stablecoins. Historically, the regulatory regime surrounding stablecoins has been characterized by uncertainty and confusion. Despite this confusion, the stablecoin industry has grown rapidly, particularly by non-bank issuers. However, more recently, a number of drastic failures in the industry have highlighted the need for regulatory intervention and clarity in the space.

Current regulatory landscape for stablecoin issuance

One of the hallmarks of the regulation of stablecoins in the United States has been uncertainty regarding which federal agencies have the authority to oversee these products. This has been an issue for the broader cryptocurrency market over the past several years, in particular regarding disagreements between the Securities and Exchange Commission ("SEC") and Commodity Futures Trading Commission ("CFTC") over whether certain technologies should be regulated as securities or commodities, or both. SEC Chairman Gary Gensler has stated that crypto products "are subject to the securities laws and must work within our securities regime,"[12] while the CFTC has declared that "Bitcoin and other virtual currencies" are commodities.[13] This turf war has extended to stablecoins, with Gensler stating that many stablecoins resemble money market mutual funds and therefore could fall under SEC authority.[14] Complicating matters, certain products may be treated both as securities and as commodities, depending on the circumstances.

On June 5, 2023, the SEC sued Binance for offering and selling BUSD – its US dollar-backed stablecoin – as an unregistered security. The SEC alleged that Binance improperly marketed and touted BUSD as a profit-generating instrument by promising interest payments to investors who merely held BUSD on the Ethereum blockchain. Binance also advertised returns of up to 15 percent for users who deposited BUSD into its "Simple Earn" program – a savings-like instrument whereby Binance generated returns from staking, lending, and otherwise deploying deposited funds. Additionally, Binance and Paxos Trust Company ("Paxos") – the issuer of BUSD and custodian of its supposedly one-to-one US dollar reserves – purportedly agreed to invest the reserves underlying BUSD and split the net interest revenue earned thereon.

The potential consequences of that conduct are obvious. As of February 10, 2023, more than 16 billion BUSD were in circulation, but Binance and Paxos did not properly disclose the risks that their investment of BUSD reserves posed to BUSD holders. Risking the underlying reserves of a stablecoin can jeopardize its future viability, as Circle almost found

out in March 2023 when Silicon Valley Bank – where roughly $3.3 billion or roughly eight percent of all USDC reserves were held – collapsed following a bank run.[15] During the fallout of that collapse, Coinbase paused conversions between USDC and US dollars on its platform.[16] Ultimately, crisis was averted when Circle was eventually able to transfer those funds to another bank.

Both the SEC and CFTC agree that stablecoins need regulatory oversight to minimize risk to the financial system. Chairman Gensler has stated that stablecoins pose a unique risk to the financial system and the wider economy, likening them to "poker chips at the casino."[17] The CFTC has gone a step further, initiating enforcement actions against stablecoin issuers for violations of the Commodity Exchange Act ("CEA"). For example, the CFTC settled charges with the companies that created the stablecoin Tether for alleged misrepresentations regarding the reserves backing the stablecoin. The order against the Tether companies required them to pay a $41 million fine and cease and desist from further violations of the CEA. Additionally, the CFTC has refused to yield to any attempts by the SEC to assert exclusive jurisdiction and has alleged that BUSD is a commodity in separate litigation against Binance.

Amidst this federal uncertainty from the SEC and CFTC, a variety of regulatory frameworks for stablecoin issuers have emerged at the state level. Numerous States currently regulate virtual currency activity through their money transmission laws, though few offer specific guidance regarding stablecoins. Texas is one notable exception, having taken the position for years now that stablecoins backed by a sovereign currency are regulated by its money transmission laws because they "may be considered a claim that can be converted into currency and thus fall within the definition of money or monetary value" under Texas law.[18] Another option for stablecoin issuers is to operate as a state-chartered trust company, such as a limited purpose trust company under the New York Banking Law.[19] Other States, such as Nebraska,[20] have options for companies to receive limited licenses or charters for stablecoin activities as well. Furthermore, some federally insured banks have announced plans to issue stablecoins under the assumption that they are within the scope of products they have the authority to issue. Importantly, traditional bank protections – like FDIC insurance, for instance – do not cleanly cover stablecoins. Paxos makes clear that, while the primary deposit account that holds fiat cash reserves is FDIC insured, "USD Stablecoins themselves are not FDIC insured." As discussed below in "Recent movements towards regulatory clarity," this authority was confirmed by the Office of the Comptroller of the Currency ("OCC"), then later partially walked back to require pre-authorization by banks before engaging in these activities.[21]

Stablecoins in action: early successes and recent failures

Despite regulatory uncertainty, several examples of successful use and issuance of stablecoins have emerged in recent years. For example, J.P. Morgan issued a coin, the JPM Coin, which is used to settle payments between clients. Its first successful test repo transaction was completed in December 2020.[22] Both the collateral and cash legs of the repo transactions were settled using blockchain technology, with the cash leveraging the JPM Coin. JPM Coin is not money *per se*. Rather it is a digital coin representing US dollars held in designated accounts. In short, a JPM Coin always has a value equivalent to one US dollar. When one client sends money to another over the blockchain, JPM Coins are transferred and instantaneously redeemed for the equivalent amount of US dollars, reducing the typical settlement time.

An even more recent example of success in the banking world is the USDF Consortium, launched in January 2022.[23] The Consortium is an association of FDIC-insured financial institutions aiming to build a network of banks to further the adoption and interoperability of the bank-minted stablecoin USDF. The goal of USDF is to facilitate the compliant transfer of value on the blockchain, removing friction in the financial system and unlocking the financial opportunities that blockchain and digital transactions can provide to a greater network of users.

There have been successes for non-bank issuers as well, which includes the largest stablecoins by market capitalization. Despite being subject to regulatory enforcement, as noted earlier, Tether has maintained its dominant status and is currently the largest stablecoin by market capitalization as of the date of this chapter.[24] Circle, the company responsible for issuing USDC, manages the second largest.[25] Other non-bank stablecoin issuers have had mixed success in the industry, such as Paxos and Gemini, which operate through limited purpose trust companies. For instance, in February 2023, Paxos, a New York-licensed limited purpose trust company, was ordered to cease issuing BUSD by the New York Department of Financial Services ("DFS") following reports that it was involved in an ongoing SEC investigation.[26]

More recently, however, PayPal announced, in partnership with Paxos, the launch of PayPal USD ("PYUSD"), a stablecoin that is "fully backed by U.S. dollar deposits, short-term U.S. treasuries and similar cash equivalents, and can be redeemed 1:1 for U.S. dollars."[27] PayPal holds a DFS-issued BitLicense. PayPal users can purchase and redeem PYUSD either within the PayPal app or directly with Paxos.[28] Only "Member Token Holders" may redeem PYUSD directly with Paxos – "Non-Member Token Holders" may hold, use, purchase, and sell PYUSD on secondary markets, but cannot redeem PYUSD for US dollars with Paxos.[29] Thus, PYUSD holders wishing to redeem their tokens directly with Paxos must first apply for membership, after which they can "withdraw some or all of their US dollars…at any time," subject to any Paxos "impose[d] withdrawal limits" and any delays necessary to verify the customer's identity and comply with anti-money laundering procedures.[30] While most withdrawals will take less than two days to complete with Paxos, "larger withdrawals may take substantially longer to complete," and Paxos reserves the right to freeze any PYUSD (or other Paxos-issued stablecoin) holding "as deemed necessary by Paxos in its sole discretion."[31]

Despite these early successes, the need for regulation has been highlighted recently as many cryptocurrencies have experienced dramatic drops in prices that have resulted in several major bankruptcy filings and related lawsuits. Additionally, the failures of Silicon Valley Bank, Signature Bank, and Silvergate Bank – each of which maintained varying degrees of cryptocurrency connections – further shook confidence in the sector. This volatility, which has been characteristic to the crypto market, has now begun to reveal some of the systemic risks associated with these products if they fail to incorporate adequate risk management.

In one spectacular example, Terraform Labs' Terra USD collapsed in May 2022, wiping out $200 billion of value in less than 24 hours.[32] LUNA was the governance token of the Terra Blockchain Network, a delegated proof-of-stake blockchain operated for the purpose of issuing and maintaining stablecoins, namely UST – a token designed to trade for exactly $1.00 (USD). To incentivize the long-term holding and use of UST, Terraform Labs (the creator of the Terra Blockchain Network) launched Anchor – a *purportedly* low-risk, high-yield savings protocol that guaranteed a 20 percent annual yield on UST deposits.

To maintain the UST peg, the protocol used a mechanism called "seigniorage" to – at least in theory – incentivize arbitrage trading that would create countervailing upward or downward price pressure. Because UST could always be swapped in or out for exactly $1.00 worth of

LUNA on the protocol level (regardless of the market price of UST), arbitrage traders were incentivized to buy UST whenever it was below $1.00 and sell UST whenever it was above $1.00. This process worked until it did not. Once UST de-pegged in May 2022, it triggered a bank run to convert out of UST into LUNA that caused further decoupling from the peg, eventually resulting in a death spiral that crashed LUNA's price to zero.

On February 16, 2023, the SEC sued Terraform Labs and its founder, Do Kwon, for offering and selling UST and LUNA as unregistered securities. On July 31, 2023, the trial court denied Terraform Labs and Kwon's motion to dismiss, ruling that their marketing of the Anchor Protocol as a means of generating revenue was sufficient under the law to render it an investment contract and, therefore, a security.[33] While the court ruled that BUSD and other stablecoins are not securities in isolation because no "reasonable expectation of profit" attaches to a fixed-priced asset by itself, Terra's marketing and offering of equity derivatives (through the Mirror Protocol) and interest-bearing products (through the Anchor Protocol) to encourage UST "deposits" constituted unregistered securities offerings and sales.

Additional examples may be found in the recent bankruptcy filings of Voyager Digital Assets Inc. and Celsius Network LLC in July 2022. Voyager at its height had millions of customers and billions in assets.[34] However, Voyager had made sizable unsecured loans to Three Arrows Capital, a crypto hedge fund that failed after its own major bets on LUNA came undone following its collapse in May. Three Arrows' default dealt a fatal blow to Voyager, which froze customer funds on July 1 and days later filed for bankruptcy. Likewise, Celsius – a platform with more than 1.7 million users at the time it filed for bankruptcy – had $75 million in exposure to Three Arrows.

The catastrophic collapse of FTX just four months later in November 2022 dwarfed both Voyager and Celsius. FTX's collapse following a liquidity crunch and bank run after its native token, FTT, plummeted in value left the exchange with a reported $8 billion in liabilities.[35]

These examples demonstrate the ripple effects that the intense volatility of the cryptocurrency market can have on lenders, counterparties, and the broader financial ecosystem, and as a result the need for regulatory action and clarity in this space has never been greater.

What has happened and what is forthcoming for stablecoin regulation?

The lack of a comprehensive, national legal framework for stablecoins, coupled with the rapid growth of the space, has prompted lawmakers and regulators to step in to fill the gap. Over the past three years, various regulatory bodies have taken a number of steps to offer guidance related to the issuance and use of stablecoins. While the guidance generally supported the idea that stablecoin activities should be regulated on a comprehensive basis, whether within the current financial system or without, we will need to wait for future movement from lawmakers and regulators to better understand how stablecoins will fit into existing laws. One example of what a comprehensive regulatory regime for stablecoins could look like is that offered by New York.

Recent movements towards regulatory clarity

At first, the federal government strongly supported the conclusion that stablecoin issuance and adjacent services were within the existing scope of banks' authority. For example, a series of interpretive letters from the OCC affirmed the authority of national banks to conduct activities related to stablecoin issuance:

- In July 2020, the OCC issued an interpretive letter confirming the authority of a national bank to provide cryptocurrency custody services for customers, provided that the bank effectively manages the risks and complies with applicable law.[36] Notably, the

interpretive letter cited national banks' longstanding authority to provide "safekeeping and custody services for a wide variety of customer assets," and added that such functions were "well established and extensively recognized as permissible activities for national banks."[37] In concluding that providing cryptocurrency custody services "is a modern form of these traditional bank activities," the letter went on to note that "as the financial markets become increasingly technological, there will likely be increasing need for banks…to leverage new technology and innovative ways to provide traditional services on behalf of customers."[38]

- In September 2020, the OCC issued an additional interpretive letter confirming the authority of national banks to provide banking services to cryptocurrency businesses and to receive deposits from issuers of stablecoins, including deposits that constitute reserves for a stablecoin that is backed on a 1:1 basis by underlying fiat currency.[39] As was the case under the previous interpretive letter, the OCC found that providing such services constituted core banking activities in which national banks are free to engage, subject to effective risk management and compliance with applicable law.
- In January 2021, the OCC issued a third interpretive letter in which it concluded that stablecoin-related activities fall within the national banking framework, and that national banks may therefore "validate, store, and record payments transactions by serving as a node on an [independent node verification network, or "INVN"]" and "use INVNs and related stablecoins to carry out permissible payment activities."[40]

On November 1, 2021, the President's Working Group on Financial Markets ("PWG"), the Federal Deposit Insurance Corporation ("FDIC") and the OCC collectively issued a Report on Stablecoins that further supported this position.[41] While this report did not contain any specific new rules or guidance, its recommendations had broad implications for existing stablecoin markets. The most significant and specific recommendation of the report was that Congress should enact legislation to "limit stablecoin issuance, and related activities of redemption and maintenance of reserve assets, to entities that are insured depository institutions" ("IDIs").[42] The legislation would prohibit other entities from issuing payment stablecoins. The goals of this legislation would be to address risks to stablecoin users from runs on the stablecoin, risks to the payment system, and systemic risks. The PWG's recommendation suggests both that issuing stablecoins is the kind of activity that can be fully performed by banks and that stablecoins are deposits under the Federal Deposit Insurance Act and Section 21 of the Glass-Steagall Act.[43]

However, two days later on November 23, 2021, the OCC issued another interpretive letter that, while portrayed as offering "clarification" regarding its previous three letters, was seemingly aimed to limit the ability of national banks to engage in crypto-related banking activities by requiring the written approval of the OCC prior to a national bank engaging in such activities.[44] In this letter, the OCC set out a process by which a national bank should notify its supervisory office in writing of its intention to engage in crypto activities. The national bank may not engage in such activities until it receives written notification of the non-objection to its plans by the supervisory office. To obtain such clearance, a national bank must demonstrate that it has adequate systems in place to identify, measure, monitor and control the risks of the activity on an ongoing basis. Risks that must be identified with respect to cryptocurrency activities include, but are not limited to, (i) operational risk, (ii) liquidity risk, (iii) strategic risk, and (iv) compliance risk.[45] Areas that will raise concerns include compliance with the Bank Secrecy Act, anti-money laundering, sanctions and consumer protection laws, and "the specific conditions, processes and controls" discussed in the earlier OCC letters.[46] The supervisory office will determine whether an activity

would be conducted in a safe and sound manner through an evaluation – not limited to cryptocurrency activities – of the adequacy of a national bank's risk management systems and controls, risk measurement systems, and other related criteria.[47] As of the date of this writing, the OCC has not publicly granted any approvals under this letter.

Similarly, the FDIC issued an industry letter in April 2022 announcing that FDIC-supervised institutions must notify the FDIC if they intend to engage in, or are currently engaged in "crypto-related activities," which include the issuance of stablecoins or holding of stablecoin reserves.[48] Institutions are required to provide the FDIC with information necessary to "allow the FDIC to engage with the institution regarding related risks."[49] The FDIC cited the various risks associated with crypto activities, including anti-money laundering and consumer protections concerns, as justifying this requirement.

On October 3, 2022, the Financial Stability Oversight Council ("FSOC") released its Report on Digital Asset Financial Stability Risks and Regulation.[50] In its report, the FSOC highlighted potential run risks and issues with stablecoin reserve assets as potential sources of financial instability if not properly addressed, citing specifically the Terra USD collapse earlier that year. The report also highlighted the risks arising from the lack of a clear regulatory framework for stablecoins, recalling the problems faced during the free banking era in the 1800s.

On January 21, 2023, the Federal Reserve, the FDIC, and the OCC issued an Interagency Statement on "Crypto-Asset Risks to Banking Organizations," which appears to signal the adoption of a more consistent approach among the federal bank regulators to concerns about safety and soundness requirements for new crypto-asset activities.[51] The statement highlighted the concerns these agencies have about risks to banking institutions in light of the recent volatility in the crypto-asset markets. The risks identified in the statement include, among other things, legal uncertainties related to custody practices, redemptions, and ownership rights, safety and soundness, fraud and misrepresentation, contagion, and stablecoin run risk.[52] The agencies also cited heightened risks associated with open, public, and/or decentralized networks, or similar systems, including, but not limited to: the lack of governance mechanisms establishing oversight of the system; the absence of contracts or standards to clearly establish roles, responsibilities, and liabilities; and vulnerabilities related to cyber-attacks, outages, lost or trapped assets, and illicit finance.[53]

On January 27, 2023, the White House's National Economic Council ("Administration") released "The Administration's Roadmap to Mitigate Cryptocurrencies' Risks."[54] The announcement emphasized the need to effectively regulate crypto-assets to protect investors, hold bad actors accountable, and prevent turmoil in the cryptocurrency sector from spreading to the broader financial system, with specific reference made to the collapse of Terra USD in May 2022. The Administration encouraged regulators to continue their efforts to clarify regulatory ambiguity and limit financial institutions' exposure to the risks of cryptocurrencies while noting that additional efforts are needed. The announcement unveiled the Administration's plan to release digital assets research and development priorities and further called for Congressional action to expand regulators' powers to prevent the misuse of customer assets, strengthen crypto-asset company disclosure requirements, and provide more severe penalties for violations of illicit finance rules.

On August 8, 2023, the Federal Reserve issued two Supervision and Regulation Letters, 23-7 and 23-8, which provided further insight into its approach to stablecoin-related activities.[55] In letter 23-7, the Federal Reserve announced the creation of a "Novel Activities Supervision Program", which, among other things, would focus on bank participation in "crypto-asset related activities", which includes "stablecoin/dollar token issuance or

distribution." The new program was established "to ensure that the risks associated with innovation are appropriately addressed" and will "enhance the supervision" of stablecoin activities conducted by banks supervised by the Federal Reserve.[56] In letter 23-8, the Federal Reserve clarified that the supervisory non-objection process laid out in the OCC's 2020 Interpretive Letters also applied to state member banks. Therefore, state member banks wishing to engage in stablecoin-related activities need to show "controls in place to conduct the activity in a safe and sound manner." State member banks also must receive a written notification of non-objection from the Federal Reserve before engaging in those activities. If a bank receives approval, the Federal Reserve will continue to subject it to "supervisory review" and "heightened monitoring of these activities."

This series of events highlights the continued lack of clarity from regulators as to whether and how financial institutions may engage in stablecoin activities. Together, these actions denote an effort by federal agencies to consolidate their regulatory posture with regard to stablecoin activities in the absence of legislative direction.[57] As a result of such efforts, banks are faced with a limited set of stablecoin activities in which they may engage, most of which are subject to pre-approval or non-objection by federal agencies.[58]

Pending legislation offers potential for future regulation

Another source of potential future clarity may arrive from legislation that has been introduced in Congress to create a comprehensive framework for the regulation of stablecoins. For example, in June 2022, Senators Kirsten Gillibrand and Cynthia Lummis introduced the bipartisan Responsible Financial Innovation Act.[59] This draft legislation defines and creates requirements for payment stablecoins aimed at promoting these new technologies while protecting consumers and markets. The bill would require the issuers of these stablecoins to "maintain high-quality liquid assets…equal to not less than 100 percent of the face amount" of the issued stablecoins' value.[60] "High-quality" assets are defined as US currency, Treasury bonds, Federal Reserve deposit balances, and other cash-like instruments. The bill also sets forth optional frameworks for banks and credit unions to issue payment stablecoins and creates an authorization for special depository institution charters under both state law and the National Bank Act to issue payment stablecoins. There is no requirement in the bill for all payment stablecoin issuers to become insured depository institutions.

An updated version of the bill was reintroduced in the Senate in July 2023.[61] The updated bill clarified that stablecoins would be governed by state and federal bank regulators and would mainly be issued by depository institutions as neither commodities nor securities. However, the bill does provide a path for institutions seeking to issue only stablecoins to receive a limited charter from the OCC for that issuance. Notably, the new bill states that algorithmic stablecoins would be considered hybrid instruments that are regulated by the CFTC. Furthermore, under the updated bill, issuers of algorithmic stablecoins would be prohibited from calling these products "stablecoins."

Stablecoin legislation has also been making its way through the House of Representatives. House Republicans, led by Representative Patrick McHenry, introduced the Clarity for Payment Stablecoins Act, which recently passed through the House Financial Services Committee, largely along party lines.[62] The new legislation would exclude payment stablecoins from the definition of securities under the securities laws and limit their issuance to entities that received permission from the appropriate regulatory authority, which may be the OCC, Federal Reserve, or applicable state regulatory authority. Non-bank issuers would face bank-like requirements, such as capital, liquidity, and risk management requirements. The bill excludes from its reach digital assets created by banks that represent deposits, and

it would also enact a two-year moratorium on the creation of new algorithmic stablecoins (referred to as "endogenously collateralized stablecoins") while directing the Treasury to conduct further research on them.

New York stablecoin regulation offers a glimpse into the future of federal regulation

While the federal government continues to develop possible approaches to stablecoin regulation, more progress has been made by States. One example of what a comprehensive regulatory framework for stablecoins may look like comes from New York. On June 8, 2022, the DFS issued its *Guidance on the Issuance of U.S. Dollar-Backed Stablecoins* ("DFS Guidance"), which outlined general requirements for USD-backed stablecoins issued by issuers subject to DFS oversight.[63] The DFS Guidance focused on three areas of requirements: redeemability; reserves; and attestations.

- As to redeemability, the DFS Guidance requires, among other things, that stablecoin issuers adopt "clear, conspicuous redemption policies, approved in advance by DFS in writing" that confer to holders the right to timely redemption of the stablecoin at par. The DFS Guidance defines "timely" redemption as occurring not more than two business days after the redemption order, though a possible exception to this requirement may apply if DFS "concludes that timely redemption would likely jeopardize the Reserve's asset-backing requirement or the orderly liquidation of Reserve assets."
- As to reserves, the DFS Guidance requires that a stablecoin be fully backed by reserve assets, which may consist only of: (1) short-term Treasury bills; (2) reverse repurchase agreements with approved counterparties; (3) government money market funds subject to DFS-approved caps; and (4) deposit accounts at US state or federally chartered depository institutions subject to DFS-approved restrictions on the amounts permitted to be held at any given institution. The DFS also expects issuers to manage liquidity risks so that the market value of the reserve assets is at least equal to the value of outstanding stablecoin units at the end of each business day.
- As to attestation, the DFS Guidance requires the issuer to release monthly reports conducted by an independent, US licensed certified public accountant ("CPA") to DFS and the public with details as to (1) the value and makeup of the reserve, (2) the outstanding stablecoin units, (3) whether the reserve is adequate to fully back the outstanding stablecoin units, and (4) whether all DFS conditions on the reserve are met. The DFS Guidance also requires that issuers obtain a yearly report attesting to management's claims regarding the effectiveness of the internal controls, structure, and procedures for compliance with the requirements of the monthly report to deliver to DFS within 120 days of the covered period, though the issuer does not need to release this report publicly.

Conclusion

This chapter has provided an overview of stablecoins and the current state of their regulation in the United States. Unfortunately, the regulatory landscape for stablecoins has been anything but stable. However, we argue that a clear path forward does exist. Banks should be permitted to engage with these technologies within existing banking laws, which already possess comprehensive systems for mitigating risk to both consumers and the broader financial system.[64] Non-bank issuers should be subject to comprehensive regulatory and supervisory regimes that are at least as thorough as those to which banks are subject. We expect significant movement towards comprehensive regulation over the next year. The future of stablecoin regulation remains uncertain, but we can be sure that this emerging technology will continue to grow.

Endnotes

1. *See* Katherine Greifeld, *Stablecoins Soar in value as Bitcoin (BTC) and everything else in Crypto Shrink*, Bloomberg (2022), available at https://www.bloomberg.com/news/articles/2022-02-24/stablecoins-soar-in-value-as-everything-else-in-crypto-shrinks (last visited Aug. 16, 2023).
2. *See* Will Canny, *Stablecoin Market to Soar to Almost $3T in Next 5 Years: Bernstein*, CoinDesk (Aug. 9, 2023), available at https://www.coindesk.com/markets/2023/08/09/stablecoin-market-to-grow-to-almost-3t-in-next-5-years-bernstein (last visited Oct. 2, 2023).
3. BitUSD, a USD-collateralized digital asset, is generally recognized as having emerged as the first stablecoin in July 2014. *See* Daniel Larimer, Charles Hoskinson, Stan Larimer, *BitShares: A Peer-to-Peer Polymorphic Digital Asset Exchange (P2P-PDAE)*, available at https://blog.bitmex.com/wp-content/uploads/2018/06/173481633-BitShares-White-Paper.pdf (last visited Aug. 16, 2023).
4. *See* Gemini, *What are stablecoins and how do they work?*, available at https://www.gemini.com/cryptopedia/what-are-stablecoins-how-do-they-work#section-how-do-stablecoins-work (last visited Aug. 16, 2023).
5. *See* CoinMarketCap, *Top Stablecoin Tokens by Market Capitalization*, available at https://coinmarketcap.com/view/stablecoin (last visited Aug. 16, 2023).
6. *See USD coin (USDC)*, Circle, available at https://www.circle.com/en/usdc (last visited Aug. 16, 2023).
7. *See* Paxos, *Pax gold – the safest way to own gold* (2022), available at https://paxos.com/paxgold (last visited Aug. 16, 2023).
8. *See* Baughman, Garth, and Jean Flemming (2020), "Global Demand for Basket-Backed Stablecoins," Finance and Economics Discussion Series 2020-048. Washington: Board of Governors of the Federal Reserve System, available at https://doi.org/10.17016/FEDS.2020.048 (last visited Aug. 16, 2023).
9. At the time of writing, Web3 remains a somewhat nebulous concept. Most articulations of the imagined future iteration of the internet include decentralization, blockchain-based decentralized applications ("dApps"), tokenization, and user ownership of data as central concepts. *See* Bobby Allyn, *People are talking about web3. Is it the internet of the future or just a buzzword?*, NPR (2021), available at https://www.npr.org/2021/11/21/1056988346/web3-internet-jargon-or-future-vision (last visited Aug. 16, 2023).
10. *See* PYMNTS.com, *Amid Collapses, Stablecoin Woes Follow a Pattern* (2022), available at https://www.pymnts.com/cryptocurrency/2022/another-hack-another-collapse-as-stablecoin-woes-follow-familiar-pattern (last visited Aug. 16, 2023).
11. *See* Bobbie Gossage, *Panics and death spirals: A history of failed stablecoins*, Fast Company (2022), available at https://www.fastcompany.com/90751716/panics-and-death-spirals-a-history-of-failed-stablecoins (last visited Aug. 16, 2023).
12. *See* U.S. Sec. & Exch. Comm'n Chair Gary Gensler, Remarks Before the Aspen Security Form (Aug. 3, 2021), available at https://www.sec.gov/news/public-statement/gensler-aspen-security-forum-2021-08-03 (last visited Aug. 16, 2023).
13. *See In re Coinflip, Inc., d/b/a Derivabit, and Francisco Riordan*, CFTC No. 15-29 (Sept. 17, 2015), available at https://www.cftc.gov/sites/default/files/idc/groups/public/@lrenforcementactions/documents/legalpleading/enfcoinfliprorder09172015.pdf (last visited Aug. 16, 2023).

14. *See* U.S. Sec. & Exch. Comm'n Chair Gary Gensler, Prepared Remarks of Gary Gensler on Crypto Markets Penn Law Capital Markets Association Annual Conference (April 4, 2022), available at https://www.sec.gov/news/speech/gensler-remarks-crypto-markets-040422 (last visited Aug. 16, 2023). The Federal Reserve also recently stepped into this conversation. Federal Reserve Chairman Jerome Powell remarked that "[w]e think that if there is private money created across the country, really there needs to be a federal role," and that "[i]n the case of [stablecoins], which is money creation, we think it really should be the Fed that plays that role." *See* Jack Denton, *Fed's Powell Eyes Oversight of Stablecoin Issuers, Regulation of Crypto Wallets*, *Barron's* (Sept. 27, 2022), available at https://www.barrons.com/articles/fed-jerome-powell-crypto-stablecoin-51664286869? (last visited Aug. 16, 2023).
15. Team Circle, *An Update on USDC and Silicon Valley Bank*, available at https://www.circle.com/blog/an-update-on-usdc-and-silicon-valley-bank (last visited Aug. 16, 2023).
16. Danny Nelson, *Coinbase Pauses Conversions Between USDC and U.S. Dollars as Banking Crisis Roils Crypto*, CoinDesk (March 10, 2023), available at https://www.coindesk.com/business/2023/03/11/coinbase-pauses-conversions-between-usdc-and-us-dollars-as-banking-crisis-roils-crypto (last visited Aug. 16, 2023).
17. *See* Tory Newmyer, *SEC's Gary Gensler likens stablecoins to 'poker chips' amid call for tougher crypto regulation*, *The Washington Post* (Sept. 21, 2021), available at https://www.washingtonpost.com/business/2021/09/21/sec-gensler-crypto-stablecoins (last visited Aug. 16, 2023).
18. *See* Texas Dep't of Banking, Supervisory Memorandum 1037 (April 1, 2019), available at https://www.dob.texas.gov/public/uploads/files/consumer-information/sm1037.pdf (last visited Aug. 16, 2023).
19. The New York Department of Financial Services ("DFS") maintains a list of regulated entities with such limited charters, including Gemini Trust Company, LLC, Paxos Trust Company, LLC, and BitGo New York Trust Company LLC. *See* New York Dep't Fin. Serv., Virtual Currency Business Activity – Regulated Entities, available at https://www.dfs.ny.gov/virtual_currency_businesses (last visited Aug. 16, 2023).
20. *See* Nebraska Legislature, Nebraska Revised Statute 8-3204, available at https://nebraskalegislature.gov/laws/statutes.php?statute=8-3024 (last visited Aug. 16, 2023).
21. A number of ancillary regulatory issues, such as those arising from "Know Your Customer" ("KYC") and anti-money laundering ("AML") regulations, are also relevant to stablecoin issuers but beyond the scope of this chapter.
22. *See* Matthew Leising, *JPMorgan Using Blockchain to Move Billions in Repo-Market Trades*, Bloomberg (Dec. 10, 2020), available at https://www.bloomberg.com/news/articles/2020-12-10/jpmorgan-using-blockchain-to-move-billions-in-repo-market-trades (last visited Aug. 16, 2023).
23. *See* USDF Consortium, *USDF ConsortiumTM Launches to Enable Banks to Mint USDF Stablecoins*, PR Newswire, available at https://www.prnewswire.com/news-releases/usdf-consortium-launches-to-enable-banks-to-mint-usdf-stablecoins-301458911.html (last visited Aug. 16, 2023).
24. *See* CoinMarketCap, *Top Stablecoin Tokens by Market Capitalization*, available at https://coinmarketcap.com/view/stablecoin (last visited Aug. 16, 2023).
25. *USD coin (USDC)*, Circle, available at https://www.circle.com/en/usdc (last visited Aug. 16, 2023).
26. Jamie Crawley, *Paxos to Stop Minting Stablecoin BUSD Following Regulatory Action*, CoinDesk (Feb. 13, 2023), available at https://www.coindesk.com/business/2023/02/13/paxos-to-stop-minting-stablecoin-busd-following-regulatory-action (last visited Aug. 16, 2023).

27. *See* PayPal, *PayPal Launches U.S. Dollar Stablecoin*, available at https://newsroom.paypal-corp.com/2023-08-07-PayPal-Launches-U-S-Dollar-Stablecoin (last visited Aug. 16, 2023).
28. *See* PayPal, *PayPal Cryptocurrency Terms and Conditions – PYUSD Stablecoin*, available at https://www.paypal.com/us/legalhub/cryptocurrencies-tnc?locale.x=en_US (last visited Aug. 16, 2023).
29. *See* Paxos, *US Dollar-Backed Stablecoin Terms and Conditions*, available at https://paxos.com/2019/03/29/usdp-terms-conditions (last visited Aug. 16, 2023).
30. *Id.*
31. *Id.*
32. *See* Low De Wei, *More Than $200 Billion Wiped Off Cryptocurrency Market in a Day*, Bloomberg (May 12, 2022), available at https://www.bloomberg.com/news/articles/2022-05-12/more-than-200-bilion-wiped-off-cryptocurrency-market-in-a-day (last visited Aug. 16, 2023).
33. *Sec. & Exch. Comm'n v. Terraform Labs Pte. Ltd.*, No. 23-CV-1346 (JSR), 2023 WL 4858299 (S.D.N.Y. July 31, 2023).
34. *See* Danny Nelson and David Z. Morris, *Behind Voyager's Fall: Crypto Broker Acted Like a Bank, Went Bankrupt*, CoinDesk (July 12, 2022), available at https://www.coindesk.com/layer2/2022/07/12/behind-voyagers-fall-crypto-broker-acted-like-a-bank-went-bankrupt (last visited Aug. 16, 2023).
35. David Yaffe-Bellany, *Embattled Crypto Exchange FTX Files for Bankruptcy*, *The New York Times* (Nov. 11, 2022), available at https://www.nytimes.com/2022/11/11/business/ftx-bankruptcy.html (last visited Aug. 16, 2023).
36. *See* Interpretive Letter #1170, OCC (July 22, 2020), available at https://www.occ.gov/topics/charters-and-licensing/interpretations-and-actions/2020/int1170.pdf (last visited Aug. 4, 2023).
37. *See* Interpretive Letter #1170, OCC (July 22, 2020), available at https://www.occ.gov/topics/charters-and-licensing/interpretations-and-actions/2020/int1170.pdf (last visited Aug. 4, 2023).
38. *See* Interpretive Letter #1170, OCC (July 22, 2020), available at https://www.occ.gov/topics/charters-and-licensing/interpretations-and-actions/2020/int1170.pdf (last visited Aug. 4, 2023).
39. *See* Interpretive Letter #1172, OCC (Sept. 21, 2020), available at https://www.occ.treas.gov/topics/charters-and-licensing/interpretations-and-actions/2020/int1172.pdf (last visited Aug. 4, 2023). On September 21, 2020, the SEC staff issued a statement regarding this interpretive letter, emphasizing that the question of whether a particular digital asset (including a stablecoin) is a security under the federal securities laws is "inherently a facts and circumstances determination." *See* U.S. Sec. & Exch. Comm'n, SEC FinHub Staff Statement on OCC Interpretation (Sept. 21, 2020), available at https://www.sec.gov/news/public-statement/sec-finhub-statement-occ-interpretation#:~:text=The%20OCC%20has%20limited%20its,redemption%20request%20to%20the%20issuer (last visited Aug. 4, 2023).
40. *See* Interpretive Letter #1174, OCC (Jan. 4, 2021), available at https://www.occ.treas.gov/topics/charters-and-licensing/interpretations-and-actions/2021/int1174.pdf (last visited Aug. 4, 2023); *see also* White & Case LLP, *Stabilized: OCC settles debate about regulatory characterization of bank-issued stablecoins* (Jan. 21, 2021), available at https://www.whitecase.com/insight-alert/stabilized-occ-settles-debate-about-regulatory-characterization-bank-issued (last visited Aug. 4, 2023).

41. President's Working Group on Financial Markets, the Federal Deposit Insurance Corporation, and the Office of the Comptroller of the Currency, *Report on Stablecoins* (Nov. 2021), available at https://home.treasury.gov/system/files/136/StableCoinReport_Nov1_508.pdf (last visited Aug. 4, 2023).
42. President's Working Group on Financial Markets, the Federal Deposit Insurance Corporation, and the Office of the Comptroller of the Currency, *Report on Stablecoins* (Nov. 2021), available at https://home.treasury.gov/system/files/136/StableCoinReport_Nov1_508.pdf (last visited Aug. 4, 2023).
43. 12 U.S.C. § 378 (2021); *see also* White & Case LLP, *Unstable: the PWG's Report on Stablecoins* (Nov. 12, 2021), available at https://www.whitecase.com/insight-alert/unstable-pwgs-report-stablecoins (last visited Aug. 4, 2023).
44. *See* Interpretive Letter #1179, OCC (Nov. 18, 2021), available at https://www.occ.treas.gov/topics/charters-and-licensing/interpretations-and-actions/2021/int1179.pdf (last visited Aug. 4, 2023).
45. *See* Interpretive Letter #1179, OCC (Nov. 18, 2021), available at https://www.occ.treas.gov/topics/charters-and-licensing/interpretations-and-actions/2021/int1179.pdf (last visited Aug. 4, 2023).
46. *See* Interpretive Letter #1179, OCC (Nov. 18, 2021), available at https://www.occ.treas.gov/topics/charters-and-licensing/interpretations-and-actions/2021/int1179.pdf (last visited Aug. 4, 2023).
47. *See* White & Case LLP, *UnSound: OCC IL 1179 and Its Backward Creation of New Law* (Dec. 1, 2021), available at https://www.whitecase.com/insight-alert/unsound-occ-il-1179-and-its-backwards-creation-new-law (last visited Aug. 4, 2023).
48. *See* Notification of Engaging in Crypto-Related Activities, FDIC (April 7, 2022), available at https://www.fdic.gov/news/financial-institution-letters/2022/fil22016.html#letter (last visited Aug. 4, 2023).
49. *See* Notification of Engaging in Crypto-Related Activities, FDIC (April 7, 2022), available at https://www.fdic.gov/news/financial-institution-letters/2022/fil22016.html#letter (last visited Aug. 8, 2023).
50. *See* Report on Digital Asset Financial Stability Risks and Regulation, FSOC (Oct. 3, 2022), available at https://home.treasury.gov/system/files/261/FSOC-Digital-Assets-Report-2022.pdf (last visited Aug. 14, 2023).
51. *See* Joint Statement on Crypto-Asset Risks to Banking Organizations (Jan. 3, 2023), available at https://www.occ.treas.gov/news-issuances/news-releases/2023/nr-ia-2023-1a.pdf (last visited Aug. 8, 2023); *see also* Douglas Landy, Glen R. Cuccinello, Leel Sinai & Chanté Eliaszadeh, *A New "Operation Choke Point"? The Quickly Constricting Rules on Crypto Activities for Banks* (May 2023), in *The Banking Law Journal*, Volume 140, available at https://www.whitecase.com/sites/default/files/2023-05/douglas-landy-glen-cuccinello-leel-sinai-chante-eliaszadeh.pdf (last visited Aug. 8, 2023).
52. *See* Joint Statement on Crypto-Asset Risks to Banking Organizations (Jan. 3, 2023), available at https://www.occ.treas.gov/news-issuances/news-releases/2023/nr-ia-2023-1a.pdf (last visited Aug. 8, 2023).
53. *See* Joint Statement on Crypto-Asset Risks to Banking Organizations (Jan. 3, 2023), available at https://www.occ.treas.gov/news-issuances/news-releases/2023/nr-ia-2023-1a.pdf (last visited Aug. 8, 2023).
54. *See* The Administration's Roadmap to Mitigate Cryptocurrencies' Risks, available at https://www.whitehouse.gov/nec/briefing-room/2023/01/27/the-administrations-roadmap-to-mitigate-cryptocurrencies-risks (last visited Aug. 8, 2023).

55. *See* Federal Reserve, SR 23-7, Creation of Novel Activities Supervision Program, available at https://www.federalreserve.gov/supervisionreg/srletters/SR2307.htm (last visited Aug. 14, 2023); Federal Reserve, SR 23-8, Supervisory Nonobjection Process for State Member Banks Seeking to Engage in Certain Activities Involving Dollar Tokens, available at https://www.federalreserve.gov/supervisionreg/srletters/SR2308.htm (last visited Aug. 9, 2023).
56. The Federal Reserve's increasing concerns about the risks of stablecoins are highlighted by a recent report comparing stablecoin risks to those associated with money market funds. *See* Kenechukwu Anadu *et al.*, Federal Reserve Bank of New York Staff Report No. 1073 (September 2023), *Runs and Flights to Safety: Are Stablecoins the New Money Market Funds?*
57. *See* Douglas Landy, Glen R. Cuccinello, Leel Sinai & Chanté Eliaszadeh, *A New "Operation Choke Point"? The Quickly Constricting Rules on Crypto Activities for Banks* (May 2023), in *The Banking Law Journal*, Volume 140, available at https://www.whitecase.com/sites/default/files/2023-05/douglas-landy-glen-cuccinello-leel-sinai-chante-eliaszadeh.pdf (last visited Aug. 8, 2023).
58. Congress also has noted the negative impacts of letters 23-7 and 23-8 on financial institutions' ability to participate in the digital asset ecosystem. Three members of the House Financial Services Committee recently wrote a letter to the Federal Reserve stating their concerns about the letters and requesting additional information and documents. *See* Letter to Jerome Powell from Patrick McHenry, French Hill & Bill Huizenga (Aug. 23, 2023), available at https://financialservices.house.gov/uploadedfiles/2023-08-23_mchenry_hill_huizenga_letter_to_fed_sr23-7_sr23-8__final.pdf (last visited Aug. 31, 2023).
59. *See* Lummis, Gillibrand Introduce Landmark Legislation to Create Regulatory Framework for Digital Assets (June 7, 2022), available at https://www.lummis.senate.gov/press-releases/lummis-gillibrand-introduce-landmark-legislation-to-create-regulatory-framework-for-digital-assets (last visited Aug. 8, 2023).
60. *See* Lummis-Gillibrand Responsible Financial Innovation Act, SIL22785 § 601, available at https://www.lummis.senate.gov/wp-content/uploads/Lummis-Gillibrand-Responsible-Financial-Innovation-Act-S.4356.pdf (last visited Aug. 8, 2023).
61. *See* Lummis-Gillibrand Responsible Financial Innovation Act, SIL23182, available at https://www.lummis.senate.gov/wp-content/uploads/Lummis-Gillibrand-2023.pdf (last visited Aug. 8, 2023).
62. *See* Clarity for Payment Stablecoins Act of 2023, available at https://www.congress.gov/118/meeting/house/116295/documents/BILLS-118-HR4766-M001156-Amdt-3.pdf (last visited Aug. 14, 2023).
63. *See* New York Dep't Fin. Serv., Virtual Currency Guidance (June 8, 2022), available at https://www.dfs.ny.gov/industry_guidance/industry_letters/il20220608_issuance_stablecoins#ftn3 (last visited Aug. 8, 2023).
64. *See Marine Bank v. Weaver*, 455 U.S. 551 (1982).

* * *

Disclaimer

Any views expressed in this publication are strictly those of the authors and should not be attributed in any way to White & Case LLP.

Douglas Landy
Tel: +1 212 819 8814 / Email: dlandy@whitecase.com

Doug is one of the most preeminent US lawyers advising financial institutions on blockchain and crypto matters. He represents global banks on the creation of blockchain and crypto trading platforms, custody, payment systems, stablecoins and related financial products. Doug has also been advising non-bank Fintech companies on potential bank charters, including the OCC's Payment Charter, and similar charters and licenses.

Clients benefit from his deep understanding of banking and securities laws, along with his thorough and practical legal analysis. He has represented banks in some of the largest M&A transactions in banking history, and in some of the most significant regulatory and Fintech events of the last two decades.

Leel Sinai
Tel: +1 212 819 2551 / Email: le-el.sinai@whitecase.com

Leel is an associate in White & Case's global Financial Services Regulatory and Fintech practices, based in the New York office. Leel has diverse experience working in-house and as a regulatory consultant. His practice focuses on bank and financial services regulation and Fintech, including innovation in cryptocurrency and payments.

Advising some of the largest financial institutions and Fintech companies, Leel provides deep regulatory expertise in connection with US federal and state bank regulatory frameworks, the application and licensing processes for regulated transactions or product offerings, as well as transaction diligence and execution for significant acquisitions and offerings. He routinely counsels clients on the strategic design and implementation of enhanced regulatory compliance and risk management programs.

Stephen Hogan-Mitchell
Tel: +1 212 819 7634 / Email: stephen.hogan-mitchell@whitecase.com

Stephen is a litigator in White & Case's New York City office, where he represents clients in complex commercial disputes in a variety of forums, with a focus on international arbitration. Stephen also advises clients on the global regulatory landscape for digital asset projects.

Chanté Eliaszadeh
Tel: +1 213 620 7893 / Email: chante.eliaszadeh@whitecase.com

Chanté is an associate in White & Case's global Financial Services Regulatory and Fintech practices, based in Los Angeles. She has a wide-ranging client base in the blockchain industry, spanning multiple chains and use cases. Before entering private practice, Chanté worked for the U.S. Securities and Exchange Commission where she helped guide the Commission in developing its crypto regulatory and enforcement approaches. During law school, Chanté started the world's first and largest blockchain law club, Blockchain at Berkeley Law, which published legal research, educated lawyers, judges, and lawmakers on blockchain technology and law, and spearheaded several philanthropic endeavors.

White & Case LLP

1221 Avenue of the Americas, New York, New York 10020, USA
Tel: +1 212 819 8200 / URL: www.whitecase.com

Stoned Cats, Ripples, and Krakens, oh my! SEC regulation of digital assets by enforcement

Richard B. Levin, Kevin R. Tran & Bobby Wenner
Nelson Mullins Riley & Scarborough LLP

There is an old adage, "May you be blessed to live in interesting times". The last years have seen the failures of FTX, a fintech darling, and a number of enforcement actions by the U.S. Securities and Exchange Commission (the "**SEC**") against leading digital asset trading platforms Binance, Bittrex, and Coinbase. The SEC has also continued to pursue investigations and actions against the issuers of digital assets, including Ripple and tokens that were offered in initial coin offerings ("**ICOs**") and the issuers of non-fungible tokens ("**NFTs**"). Finally, the SEC launched and settled an enforcement action against Kraken related to the offering of a stablecoin. There is no evidence that the SEC plans to slow the pace of actions against firms in the digital asset space and we will continue to live in exciting times.

This chapter focuses on the regulation of digital assets in the United States, including: (i) the regulation of digital assets that are securities; (ii) the regulation of trading platforms that facilitate the trading of digital assets that are securities; (iii) the regulation of platforms that facilitate the clearance and settlement of digital assets that are deemed securities; and (iv) the regulation of stablecoins and staking. This chapter concludes with a discussion of the recent enforcement actions involving NFTs. To understand these issues, it is important to understand blockchain technology.

Blockchain and digital assets

Blockchain technology is the backbone of digital assets, which are intangible "asset[s] that [are] issued and transferred using distributed ledger or blockchain technology".[1] For example, cryptocurrencies and tokens are unique subsets of digital assets that utilise cryptography to assure the authenticity of digital assets by creating a secure, distributed network for transactions.[2] Although the term "digital asset" is not defined in U.S. securities laws, a digital asset may be deemed a security. The SEC refers to digital assets that are securities as a "digital asset security". To understand the regulation of digital assets that are securities, it is useful to understand blockchain technology.

Blockchain

A blockchain is a database structure that can only be updated by appending a new set (or block) of valid transactions to the log of a previous transaction.[3] In its most basic form, the blockchain records ownership of transactions involving the cryptocurrency (including Bitcoin) across a decentralised, wide network of computers where transactions are signed off by the parties involved using the software, checked by the network or the "crowd", and then added and encrypted into the blockchain without need for a "trusted middleman" to sit in between parties in a transaction.[4]

On a public (permissionless) blockchain, access to the network is unrestricted. Despite public misconceptions of the technology, public blockchains are not anonymous; they are

pseudonymous. On a public blockchain network, users can validate transactions, which ensures that all nodes are synchronised and that there is consensus regarding the legitimacy. Consensus is required for the block to be considered immutable.[5]

Permissioned blockchain networks are based on consensus mechanisms. Only approved participants can update a permissioned blockchain. A centralised authority must determine which consensus to use, how many nodes should participate in the network, and who authorises new nodes. Furthermore, someone must determine and validate cybersecurity requirements, and decide when to upgrade and validate the code.[6]

Wallets and keys

Digital assets are stored by associating them with addresses called "wallets", which can be stored on web servers, local hardware, mobile devices, or paper printouts.[7] A digital asset wallet takes the form of a cryptographic public key, as a string of numbers and letters.[8] Each public key has a matching "private key" known only to the user.[9] Control of the private key is what assures one control of the digital assets at any address, so collections of private keys must be protected by passwords or other means of securing them.[10]

Digital asset securities

The year 2017 marked the start of a frenzy of digital asset offerings commonly known as ICOs. Unlike initial public offerings, ICOs were neither marketed with a registration with the SEC nor offered pursuant to an exemption from registration. The explosion of ICOs prompted several responses from the SEC, including an investigation conducted by the SEC regarding whether a decentralised autonomous organisation ("**DAO**") created by Slock.it UG ("**Slock.it**"), a German corporation, and Slock.it's co-founders, violated U.S. securities laws with their ICO. The ensuing investigation and report (the "**DAO Report**") found that Slock.it engaged in the sale of an unregistered security.[11] The SEC used the DAO Report as an opportunity to remind the public that all securities offered and sold in the United States must be registered with the SEC or must qualify for an exemption from the registration requirements. Additionally, any entity or person engaging in the activities of an exchange must "register as a national securities exchange or operate pursuant to an exemption from such registration".[12] Then SEC Chairman, Jay Clayton, cautioned potential investors in these ICOs that none of the ICOs were registered with or approved by the SEC,[13] thus having a chilling effect on ICOs.

While the SEC has not adopted rules specifically tailored to digital assets that are securities, Chairman Gensler has noted the importance of the SEC to provide guidance and clarity to promote blockchain technology while ensuring investor protections are maintained, including that he believes "a lot of crypto tokens – I won't call them cryptocurrencies for this moment – are indeed securities"[14] and that "Bitcoin and other cryptocurrencies brought new thinking to payments but raised new issues of investor protection we still need to attend to".[15]

What is a security?

The definitions of "security" under the Securities Act of 1933 (the "**Securities Act**") and the Securities Exchange Act of 1934 (the "**Exchange Act**") and court interpretations[16] are broad enough to include the various types of instruments that are used in commercial marketplaces that one might suspect to fall within the ordinary concepts of a security,[17] including stocks, bonds, and notes, and various collective investment pools and common enterprises.[18] The SEC has argued that investments in digital asset-related schemes are investment contracts – a contract, transaction, or scheme involving (i) an investment of money, (ii) in a common enterprise, (iii) with the expectation that profits will be derived from the efforts of the

promoter or a third party.[19] If all digital assets issued to date are securities,[20] they would be subject to existing securities laws that address the offer, sale, secondary trading, clearance and settlement of securities.

Section 2(a)(1) of the Securities Act defines a "security" as:

> [A]ny *note*, stock, treasury stock, security future, security-based swap, bond, debenture, evidence of indebtedness, certificate of interest or participation in any profit-sharing agreement, collateral-trust certificate, preorganization certificate or subscription, transferable share, *investment contract*, voting-trust certificate, certificate of deposit for a security, ... or, in general, any interest or instrument commonly known as a "security.[21]

In determining whether an instrument is a security, courts will look at the economic reality and focus on the substance rather than form.[22] In enforcement actions, the SEC has argued that offerings of digital assets are investment contracts.[23] What constitutes an investment contract is determined based on the test articulated by the U.S. Supreme Court in *SEC v. W.J. Howey Co*.

Howey test

Under the *Howey* test, an investment contract is a contract, transaction, or scheme involving (i) an investment of money, (ii) in a common enterprise, (iii) with the expectation that profits will be derived from the efforts of the promoter or a third party.

Investment of money

The SEC has taken the position that the investment does not have to take the form of "money", but it can be any "specific consideration in return for a separable financial interest with the characteristics of a security".[24] The first prong of the *Howey* test is typically satisfied in an offer and sale of a digital asset because the digital asset is purchased or otherwise acquired in exchange for value (i.e., fiat currency or another digital asset) as consideration.[25]

Common enterprise

Courts have generally analysed "common enterprise" as a distinct element of an investment contract. However, courts are divided on whether horizontal (pooling of assets from multiple investors in such a manner that all share in the profits and risks of the enterprise) or vertical commonality (an investor's fortunes are tied to the promoter's success rather than to fellow investors) is required.

Reasonable expectation of profits derived from the efforts of others

Under the *Howey* test, profits can be either capital appreciation resulting from the development of the initial investment, or a participation in earnings resulting from the use of investors' funds.[26] Profits are income or return that investors seek on their investment, not the profits of the scheme in which they invest.[27] Profits include, for example, dividends, other periodic payments, or the increased value of the investment. The determining factor under this prong of the *Howey* test is that the investor is "attracted solely by the prospects of a return" on his investment.[28] The investor may not have been motivated by a desire to use or consume the item purchased.[29] In determining whether an investor was "attracted or led" by the expectation of profits, courts look at whether the promoter has induced prospective investors with proposed or promised profits. The SEC staff have noted:

> The main issue in analyzing a digital asset under the *Howey* test is whether a purchaser has a reasonable expectation of profits (or other financial returns) derived from the efforts of others. A purchaser may expect to realize a return through participating in distributions or through other methods of realizing appreciation on the asset, such as selling at a gain in a secondary market.[30]

In addition to the *Howey* test for investment contracts, digital assets may also be deemed debt securities.

Reves test

Under the test articulated by the U.S. Supreme Court in *Reves v. Ernst & Young*, all notes are presumptively securities. However, that presumption is rebuttable in two ways. First, the seller of a note can establish that a note bears a "family resemblance" to one of the constituents of a judicially created list of notes that are not securities. In *Reves*, the court adopted the "family resemblance" test to determine whether a note is a security. Under the family resemblance test, there is a presumption that a note is a security, with the presumption being rebutted if the note bears a resemblance to one of the enumerated categories on a judicially developed list of exceptions. If the note does not bear resemblance to an item on the list, the analysis continues to determine whether a new category should be added to the list. In determining whether a note bears a resemblance to one of the enumerated exceptions to a security, or whether a new exception should be added, the courts consider: (i) the motivations and purpose of the buyer and seller in the transaction; (ii) the issuer's plan of distribution for the note; (iii) the reasonable expectations of the investing public; and (iv) the existence of an alternative regulatory scheme that sufficiently protects investors.

Motivation and purpose

The court examines the transaction to assess the motivations that would "prompt a reasonable seller and buyer to enter into [the transaction]". If the seller's purpose is to raise money for the general use of a business enterprise or to finance substantial investments and the buyer is interested primarily in the profit the note is expected to generate, the instrument is likely to be a "security". If the note is exchanged to facilitate the purchase and sale of a minor asset or consumer good, to correct the seller's cashflow difficulties, or to advance some other commercial or consumer purposes, on the other hand, the note is less likely to be a "security".

Plan of distribution

The second factor determines whether the instrument is being distributed for investment or speculation. If the note is being offered and sold to a broad segment of the public for investment purposes or for "speculation or investment", the note is likely to be a "security".

Reasonable expectations of the investing public

An instrument will be deemed a security where the reasonable expectation of the investing public is that the securities laws (and accompanying anti-fraud provisions) apply to the investment. The courts will consider instruments to be "securities" based on such public expectations, even where an economic analysis of the circumstances of the particular transaction might suggest that the instruments are not "securities" as used in the transaction.

Existence of an alternative regulatory scheme

The fourth factor is a determination of whether another regulatory scheme "significantly reduces the risk of the instrument, thereby rendering the application of the Securities Act unnecessary". The FDIC and ERISA laws are two such examples.

Application of the *Howey* and *Reves* tests

Both the *Howey* and *Reves* tests are fact-intensive. As a result, the details surrounding specific digital asset offerings may prove decisive under either inquiry. There is also some ambiguity as to when the tests apply. If a digital asset is a security, the platform facilitating the sale and secondary trading of the digital asset security may have to register with the SEC as an exchange or a broker-dealer and alternative trading system ("**ATS**").

SEC v. Ripple

On July 13, 2023, Judge Analisa Torres of the U.S. District Court for the Southern District of New York issued a decision in the SEC's case against Ripple Labs ("**Ripple**").[31] The court appeared to deliver partial victories to both the SEC and to Ripple on the parties' summary judgment motions in perhaps the most anticipated decision to date in the digital asset industry.

The blockchain "XRP Ledger" was developed in 2011 along with 100 billion XRP tokens, which is the native digital token of the XRP Ledger and is required to perform any transactions on the XRP Ledger. In 2012, one of the XRP Ledger's creators founded Ripple. Ripple's founders retained 20 billion XRP tokens for themselves and provided the remaining 80 billion XRP tokens to Ripple. Between 2013 and 2020, Ripple engaged in various sales and distributions of XRP: Ripple sold approximately $730 million worth of XRP tokens directly to third parties in private sales, including institutions and hedge funds (termed "**Institutional Sales**"); Ripple sold roughly $750 million worth of XRP tokens on digital asset exchanges using trading algorithms (termed "**Programmatic Sales**"); and Ripple distributed roughly $610 million worth of XRP as a form of payment for services (termed "**Other Distributions**"). Ripple's founders sold some or all their XRP tokens in their individual capacities (e.g., one founder sold $450 million of XRP tokens).[32]

Judge Torres ruled that Ripple's Institutional Sales of XRP to sophisticated individuals and entities pursuant to written contracts amounted to unregistered offers and sales of investment contracts in violation of Section 5 of the Securities Act. Institutional Buyers invested money by purchasing XRP tokens; horizontal commonality existed because the fortunes of each investor were tied to other investors and to Ripple; and the Institutional Buyers purchased XRP with the expectation that they would derive profits from Ripple's efforts.

Judge Torres concluded that Ripple's Programmatic Sales, which were sales of XRP by Ripple to public buyers on digital asset exchanges, did not constitute offers and sales of investment contracts because the sales were blind bid/ask transactions, and the buyers would not have known whether their payments were going to Ripple or another seller of XRP. Judge Torres held that "the economic reality is that Programmatic Buyers stood in the same shoes as a secondary market purchase who did not know to whom or what it was paying its money". Thus, there could be no reasonable expectation that the buyers would derive profits from Ripple's efforts *vis-à-vis* the funds from the XRP sale. Judge Torres further noted that "it is not enough for the SEC to argue that Ripple 'explicitly targeted speculators' or that 'Ripple understood that people were speculating on XRP as an investment' because a speculative motive 'on the part of the purchaser or seller does not evidence the existence of an 'investment contract' within the meaning of the [Securities Act]'". The court noted that someone buying a horse or a car hoping to realise a profitable investment is not buying a security because the expected return is not contingent upon the continuing efforts of someone else.

Judge Torres held that the Programmatic Buyers may have purchased XRP with an expectation of profit, "but they did not derive that expectation from Ripple's efforts (as opposed to other factors, such as general cryptocurrency market trends) – particularly because none of the Programmatic Buyers were aware that they were buying XRP from Ripple". The court explained that some Programmatic Buyers may have purchased XRP with the expectation of profits to be derived from Ripple's efforts, but that "the inquiry is an objective one focusing on the promises and offers made to investors; it is not a search for the precise motivation of each individual participant". However, despite cryptocurrency exchanges' rush to relist XRP following Judge Torres' decision (e.g., Coinbase relisted

XRP within hours), the order *does not address* whether secondary sales of XRP on third-party-operated platforms are securities or the permissibility of cryptocurrency exchanges to facilitate the purchase and sale of XRP.

Judge Torres concluded that Ripple's distribution of XRP to employees and as compensation to third parties did not amount to investment contracts because those transfers of XRP were not carried out pursuant to an "investment of money", as required under *Howey*. Ripple never received any payments from these XRP distributions, and therefore the distributions could not be investment contracts.

On August 9, 2023, the SEC staff advised Judge Torres that they planned to file a motion for leave to file an interlocutory appeal to the Second Circuit Court of Appeals with respect to the court's July 13, 2023 order granting summary judgment to the defendants. Specifically, the SEC noted that it seeks to appeal the court's holding that the defendants' "Programmatic" offers and sales to XRP buyers over crypto asset trading platforms and Ripple's "Other Distributions" in exchange for labour and services did not involve the offer or sale of securities under *Howey*. Judge Torres granted the SEC permission to file the motion for leave to file an interlocutory appeal, but then denied the motion on October 3, 2023.

On October 19, 2023, the SEC formally dropped its charges against Ripple's executives Bradley Garlinghouse and Christian Larsen in its enforcement case relating to whether either executive aided and abetted sales of XRP to institutions.

Stablecoins

SEC Chairman Gary Gensler has said: "These stablecoins are acting almost like poker chips at the casino."[33] Gensler's concerns about stablecoins echo the comments of the Presidential Working Group on Stablecoins, which noted in its report that a stablecoin "may constitute a security, commodity, and/or derivative ... subject to the U.S. federal securities laws, or ... subject to the [Commodity Exchange Act]".[34] The Presidential Working Group also noted that "[t]he federal securities laws and/or the [Commodity Exchange Act] may apply to the stablecoin, the stablecoin arrangement, transactions in, and/or participants involved in, the stablecoin or stablecoin arrangement, and/or derivatives of any of the fore- going instruments". The International Organization of Securities Commissions ("**IOSCO**") has noted that "so-called 'stablecoins' can include features that are typical of regulated securities".[35]

What is a stablecoin?

A stablecoin is a digital asset whose value is pegged, or tied, to a reference asset. The reference asset could be a currency, commodity or other financial instrument. Stablecoins are designed to maintain a stable price over time and provide an alternative to more volatile cryptocurrencies. The first stablecoin was issued in 2014 and, since then, stablecoins have risen in popularity. Stablecoins were primarily used to buy cryptocurrencies on trading platforms that did not offer fiat currency trading pairs. As adoption grew, stablecoins began to be used in several blockchain-based financial services and used to pay for goods and services. According to CoinMarketCap, the total market capitalisation of stablecoins is estimated to be approximately $152 billion.[36]

Stablecoins use different mechanisms to maintain their price peg. The two most common methods are maintaining a pool of reserve assets as collateral or using an algorithmic formula to control the supply of a coin.

Collateralised stablecoins

Collateralised stablecoins maintain a pool of collateral to support the coin's value. The types of collateral could include fiat currency, commodities or other cryptocurrencies. For

example, the issuer of a stablecoin pegged to the U.S. dollar would maintain $1 million in reserve to support 1 million units of the stablecoin. Whenever the holder of the stablecoin wishes to cash out his or her tokens, an equal amount of the collateralising asset is taken from the reserve. Another example is a crypto-backed stablecoin, which can be issued to launch one asset on a different blockchain. For example, Wrapped Bitcoin ("**WBTC**") is a stablecoin pegged to Bitcoin and issued on the Ethereum blockchain.

Algorithmic stablecoins

Algorithmic stablecoins maintain their value by controlling the stablecoin's supply through an algorithm. Coins are either destroyed (burned) or created (minted) to keep the coin's value in line with the target price. For example, if the value of a stablecoin drops from the target price of $1 to $0.75, the algorithm will automatically burn a tranche of coins to introduce more scarcity, propping up the price of the stablecoin. Alternatively, if the stablecoin's price exceeds that of the target price, new tokens are issued to bring the stablecoin's value down.

TerraUSD ("**UST**") is an example of an algorithmic stablecoin whose price is pegged at $1.00 via the minting and burning of its sister coin, LUNA. UST is not collateralised – its model operates via the algorithmic minting and burning of LUNA tokens each time a UST stablecoin is bought or sold. However, in May 2022, UST suffered the crypto equivalent of a bank run, which resulted in a "de-pegging" of UST from its $1 price and sending both the stablecoin and its sister coin close to zero.

SEC v. Terra

The decision in the *Ripple* case stands in stark contrast to a recent ruling in another case in the U.S. District Court for the Southern District of New York. In that case, the SEC alleged that Terraform Labs Pte. Ltd. and Do Hyeong Kwon orchestrated a multi-billion-dollar crypto asset securities fraud involving an algorithmic stablecoin and other crypto asset securities. According to the SEC, from April 2018 until the scheme's collapse in May 2022, Terraform and Kwon raised billions of dollars from investors by offering and selling an interconnected suite of digital asset securities, including "mAssets", which the SEC claims are security-based swaps designed to pay returns by mirroring the price of stocks of U.S. companies, and UST, a digital asset security referred to as an "algorithmic stablecoin" that supposedly maintained its peg to the U.S. dollar by being interchangeable for another of the defendants' crypto asset securities, LUNA. The SEC claims that Terraform and Kwon offered and sold investors other means to invest in their crypto empire, including the crypto asset security tokens MIR – or "mirror" tokens – and LUNA itself.

The SEC also alleged that Terraform and Kwon marketed crypto asset securities to investors seeking to earn a profit, repeatedly claiming that the tokens would increase in value. The SEC claims that while marketing the LUNA token, Terraform and Kwon repeatedly misled and deceived investors that a popular Korean mobile payment application used the Terra blockchain to settle transactions that would accrue value to LUNA. Meanwhile, Terraform and Kwon also allegedly misled investors about the stability of UST. In May 2022, UST de-pegged from the U.S. dollar, and the price of it and its sister tokens plummeted to close to zero.

Faced with the defendants' motion to dismiss and the earlier ruling by Judge Torres in the *Ripple* case, Judge Jed Rakoff elected to take a different position on the regulation of digital assets.[37] He recognised that the UST and LUNA tokens may not have qualified as "investment contracts" but noted that "this conclusion is only marginally of interest, because, to begin with the coins were never, according to the amended complaint, standalone tokens".[38] Judge Rakoff noted that the SEC had alleged that the LUNA coins were marketed as "yield-bearing

investments whose value would grow in line with the Terraform blockchain ecosystem" and that the UST coins "could be converted to LUNA coins".[39] He held that there was a plausible "common enterprise" because the defendants had broadly marketed the coins as profit-generating based on the defendants "pooling" purchasers' investments, including by investing proceeds from the sale of coins "to develop the Terraform blockchain", which the defendants allegedly held out publicly would "increase the value of the LUNA tokens themselves".[40]

Judge Rakoff "decline[d] to draw a distinction between the[] coins based on their manner of sale, such that coins sold directly to institutional investors are considered securities and those sold through secondary market transactions to retail investors are not". He rejected the approach adopted by Judge Torres in the *Ripple* case. Judge Rakoff declined "to draw a distinction between" sales of tokens to institutional investors and sales in secondary market transactions, and expressly stated that "in doing so, the court rejects the approach recently adopted by another judge of this District in a similar case, *SEC v. Ripple Labs, Inc*.".[41]

Rejecting the logic of Judge Torres, Rakoff concluded that "*Howey* makes no such distinction between purchasers. And it makes good sense that it did not. That a purchaser bought the coins directly from the defendants or, instead, in a secondary re-sale transaction has no impact on whether a reasonable individual would objectively view the defendants' actions and statements as evincing a promise of profits based on their efforts".

The *Ripple* and *Terra* cases will be of great interest to other issuers of digital assets who are facing their own SEC enforcement actions in courts across the country.

Securities exchanges, broker-dealers, and alternative trading systems

Section 3(a)(1) of the Exchange Act defines an "exchange" as "any organization, association, or group of persons, whether incorporated or unincorporated, which constitutes, maintains, or provides a marketplace or facilities for bringing together purchasers and sellers of securities or for otherwise performing with respect to securities the functions commonly performed by a stock exchange as that term is generally understood ....".[42]

Securities exchanges

Rule 3b-16(a) of the Exchange Act provides a functional test to assess whether a trading system meets the definition of exchange. Under Rule 3b-16(a), an organisation, association, or group of persons will be deemed to provide "a marketplace or facilities for bringing together purchasers and sellers of securities or for otherwise performing with respect to securities the functions commonly performed by a stock exchange" if such organisation, association, or group of persons: (i) brings together the orders for securities of multiple buyers and sellers; and (ii) uses established, non-discretionary methods (whether by providing a trading facility or by setting rules) under which such orders interact with each other, and the buyers and sellers entering such orders agree to the terms of the trade.

As the SEC noted in the DAO Report, a system that meets the definition of an exchange and is not excluded under Rule 3b-16(b) must register as a national securities exchange or operate pursuant to an appropriate exemption.[43] One frequently used exemption is for ATSs. Rule 3a1-1(a)(2) exempts from the definition of "exchange" under Section 3(a)(1) an ATS that complies with Regulation ATS. An ATS that operates pursuant to the Rule 3a1-1(a)(2) exemption and complies with Regulation ATS would not be subject to the registration requirement of Section 5 of the Exchange Act.

Alternative trading systems

In 1998, the SEC adopted Regulation ATS, which allows an ATS to choose whether to register as a national securities exchange or to register as a broker-dealer and comply with

additional requirements of Regulation ATS. An "ATS" is any organisation, association, person, group of persons, or system that: (i) constitutes, maintains, or provides a marketplace or facilities for bringing together purchasers and sellers of securities or for otherwise performing with respect to securities the functions commonly performed by a stock exchange within the meaning of Rule 3b-16 under the Exchange Act; and (ii) does not set rules governing the conduct of subscribers other than the conduct of such subscribers' trading on such organisation, association, person, group of persons, or system, or discipline subscribers other than by exclusion from trading.[44]

A digital asset platform may be required by the SEC to register as an ATS if it maintains a marketplace or facilities for bringing together purchasers and sellers of digital assets that are deemed securities, and it does not set rules governing the conduct of subscribers other than the conduct of such subscribers' trading on such platform. If the platform is not required to register as an ATS, the operator of the platform may be required to register as a broker-dealer.

Brokers and dealers

Section 15 of the Exchange Act requires registration with the SEC of all broker-dealers using interstate commerce or the facilities of any national securities exchange to effect transactions in securities (other than exempted securities and certain short-term debt instruments). Section 3(a)(4)(A) of the Exchange Act broadly defines a "broker" as "any person engaged in the business of effecting transactions in securities for the account of others". The Exchange Act and the rules thereunder do not define these terms, and the SEC and the courts apply a general "facts and circumstances" analysis in evaluating whether a person has acted as a broker.

Engaged in the business

Courts have read "engaged in the business" as connoting a certain regularity of participation in purchasing and selling activities rather than a few isolated transactions. Such "regularity of business" is determined by (i) the number of transactions and clients, and the dollar amount of securities sold, and (ii) the extent to which advertisement and investor solicitation were used. Besides "regularity of business", several other factors oftentimes indicate that a person is "engaged in the business": (i) receiving transaction-related compensation; (ii) holding oneself out as a broker, as executing trades, or as assisting others in settling securities transactions; and (iii) soliciting securities transactions.

The operator of a digital asset platform could be deemed to be engaged in the business of effecting transactions in securities because it will more than likely receive transaction-related compensation, execute trades for users of the platform, and solicit users to engage in such transactions.

Role of compensation in analysis

SEC guidance and enforcement actions have noted that the receipt of commissions or other transaction-related compensation is an important factor in deciding whether a person is a "broker" subject to the registration requirements under the Exchange Act.[45] Transaction-related compensation refers to compensation based, directly or indirectly, on the size, value, or completion of any securities transactions, which often indicates that the person is engaged in the business of effecting transactions in securities.[46]

Effecting transactions in securities

Courts and the SEC have determined that a person "effects transactions in securities" if the person participates in such transactions "at key points in the chain of distribution".[47] Participation may include: (i) assisting an issuer to structure prospective securities transactions; (ii) helping an issuer to identify potential purchasers of securities; (iii)

screening potential participants in a transaction for creditworthiness; (iv) soliciting securities transactions (including advertising); (v) negotiating between the issuer and the investor; (vi) making valuations as to the merits of an investment or giving advice; (vii) taking, routing or matching orders, or facilitating the execution of a securities transaction; (viii) handling customer funds or securities; and (ix) preparing and sending transaction confirmations (other than on behalf of a broker-dealer that executes the trades). Handling customer funds may also include handling a customer's digital currencies, like Bitcoin, in connection with Bitcoin-denominated securities transactions.[48] Accordingly, the SEC could deem a platform that is facilitating transactions in digital assets to be executing securities transactions if it is helping an issuer to identify potential purchasers of securities.

Clearing agencies

Congress directed the SEC in 1975 to facilitate the establishment of a national system for the prompt and accurate clearance and settlement of securities transactions when it added Section 17A to the Exchange Act as part of the Securities Acts Amendments.[49] At the time of the adoption of the Securities Acts Amendments, the Senate Committee on Banking, Housing, and Urban Affairs stated that the "banking and security industries must move quickly toward the establishment of a fully integrated national system for the prompt and accurate processing and settlement of securities transactions".[50]

A key component of the SEC's supervision of the securities clearance and settlement system is its authority to regulate clearing agencies. Before performing clearing agency functions, including trade comparison, netting, matching, and settlement activities, intermediaries must either register with the SEC or apply for an exemption from registration. The SEC's ability to achieve these goals and its supervision of securities clearance and settlement systems is based on the regulation of registered clearing agencies.[51]

Clearing corporations

Clearing corporations compare member transactions (or report to members the results of exchange comparison operations), clear those trades and prepare instructions for automated settlement of those trades, and often act as intermediaries in making those settlements.[52] Clearing corporations provide several essential services to the market, including comparing and confirming trade data submitted by participants (or reporting to participants the results of trade comparisons submitted by the exchanges), acting as the common counterparty and guaranteeing the completion of the trade if either side defaults or goes out of business, and preparing instructions for their participants regarding their settlement obligations. Clearing corporations generally instruct depositories to make securities deliveries that result from settlement of securities transactions.

Depositories

In 1975, Congress considered the idea of separately regulating securities depositories, but instead defined clearing agencies in Section 3(a)(23)(A) to include depositories. There are statutory exceptions in Section 3(a)(23)(B), including: (i) any national securities exchange or solely by reason of its providing facilities for comparison of data respecting the terms of settlement of securities transactions effected on such exchange or by means of any electronic system; and (ii) any bank, broker, dealer, if such bank, broker, dealer would be deemed to be a clearing agency solely by reason of functions performed by such institution as part of customary brokerage.

Depositories provide multiple services to the market by retaining custody of equity and debt securities issues and maintaining ownership records. The organisation also effects deliveries of securities between participants via a book entry system that transfers ownership of securities

electronically, thus eliminating the need for the physical movement of securities. Depositories receive instructions from the clearing corporation to deliver and receive securities on behalf of its participants, or from participants themselves, to move securities from one participant's account to another. The institutions also communicate with settling banks to net settle any financial obligations. Depositories hold securities certificates in bulk form for their participants and maintain ownership records of the securities on their own books.

In the *BTC Trading Corp.* case, the SEC concluded that the defendants had *custody and control of customer funds* by virtue of controlling the digital wallet in which the assets were stored.[53] The SEC appears to be arguing that *Coinbase* and *Binance* are acting as depositories because they are facilitating deliveries of securities between participants via the blockchain (a book entry system that transfers ownership electronically), without the need for the physical movement of securities.

Even if a blockchain technology platform is not deemed to be acting as a depository, it could be deemed to be acting as a transfer agent.

Transfer agents

A "transfer agent" is defined in Section 3(a)(25) of the Exchange Act as "any person who engages on behalf of an issuer of securities or on behalf of itself as an issuer of securities in: (i) countersigning such securities upon issuance, (ii) monitoring the issuance of such securities with a view to preventing unauthorized issuance, a function commonly performed by a person called a registrar, (iii) registering the transfer of such securities, (iv) exchanging or converting such securities, or (v) transferring record ownership of securities by bookkeeping entry without physical issuance of securities certificates". Transfer agents are required to register with the SEC. Transfer agents record changes of ownership, maintain the issuer's security holder records, cancel and issue certificates, and distribute dividends. Because transfer agents stand between issuing companies and security holders, efficient transfer agent operations are critical to the successful completion of secondary trades.

Section 17A(c) of the Exchange Act requires that transfer agents be registered with the SEC, or if the transfer agent is a bank, with a bank regulatory agency.[54] No registered self-regulatory organisation governs transfer agents.[55] The SEC has promulgated rules and regulations for all registered transfer agents, intended to facilitate the prompt and accurate clearance and settlement of securities transactions and to assure the safeguarding of securities and funds.[56] The rules include minimum performance standards regarding the issuance of new certificates and related recordkeeping and reporting rules, and the prompt and accurate creation of security holder records and the safeguarding of securities and funds. The SEC also conducts inspections of transfer agents.[57]

A blockchain technology platform could be required to register as a transfer agent if it monitors the issuance of securities or registers the transfers of securities. While it is unlikely that a blockchain technology platform would countersign securities, DAOs could be deemed to be monitoring the issuance of securities with a view to preventing unauthorised issuance (i.e., a registrar, registering the transferring of such securities). Other blockchain platforms could be deemed to be registering the transfer of securities, exchanging or converting securities, or transferring record ownership of securities by a bookkeeping or ledger entry without physical issuance of securities certifications.

SEC enforcement actions against digital asset trading platforms

The SEC has brought enforcement actions against the operators of platforms that facilitate the trading of digital assets and that host digital asset wallets.

Binance

On June 5, 2023, the SEC charged Binance (which operates the largest digital asset trading platform in the world, Binance.com), U.S.-based affiliate, BAM Trading Services, Inc. (which, together with Binance, operates the U.S.-based crypto trading platform, Binance.US), and their founder, Changpeng Zhao, with numerous securities law violations.[58] In its complaint, the SEC alleged that although Zhao and Binance publicly claimed that U.S. customers were restricted from transacting on Binance.com, Zhao and Binance "subverted their own [risk management and corporate governance] controls to allow high net worth U.S. customers to continue trading on the Binance.com platform".[59] The SEC alleged that the defendants unlawfully solicited U.S. investors to buy, sell, and trade digital asset securities through unregistered trading platforms available online at Binance.com.[60] The SEC also claims the defendants engaged in unregistered offers and sales of digital asset securities.[61] Finally, the SEC alleged that BAM Trading and BAM Management defrauded equity, retail, and institutional investors about purported surveillance and controls over manipulative trading on the Binance.US platform, which were in fact virtually non-existent.[62]

Coinbase

Following the complaint against Binance, the SEC, on the next day, charged Coinbase with operating its crypto trading platform as an unregistered national securities exchange, broker, and clearing agency.[63] According to the SEC's complaint, Coinbase has made billions since 2019 by unlawfully facilitating the buying and selling of crypto asset securities.[64] The complaint alleges that Coinbase (i) provides a marketplace that matches multiple buyers and sellers using non-discretionary methods (i.e., using technology), (ii) facilitates securities transactions for its customers, (iii) provides securities depository services, and (iv) engages in unregistered securities offerings through its staking-as-a-service programme.[65]

Of particular interest in the Coinbase complaint is the identification of numerous digital assets that the SEC has identified as securities.[66] Among those identified were Cardano, Solana, and Polygon, which, as of July 17, 2023, were the seventh, eighth, and 10th largest digital assets by market cap in the world.[67] The case is also one of the first SEC enforcement actions to allege that the platform acted as an unregistering clearing agency.

Bittrex

The SEC recently entered into a settlement with digital asset trading platform Bittrex, Inc. ("**Bittrex**") and its co-founder and former CEO, William Shihara.[68] Bittrex's foreign affiliate, Bittrex Global GmbH ("**Bittrex Global**"), also agreed to settle charges that it failed to register as a national securities exchange. The SEC alleged in the complaint filed on April 17, 2023 that Bittrex acted as an unregistered broker, exchange, and clearing agency by providing services to U.S. investors in connection with digital assets that the SEC alleged were offered and sold as securities.[69] The SEC also alleged that Bittrex and Shihara directed issuers who sought to have their digital assets made available for trading on Bittrex's platform to first delete from public channels certain "problematic statements" that Shihara believed would lead a regulator, such as the SEC, to investigate whether the digital asset was offered and sold as a security.[70]

As part of the settlement, which is subject to court approval, the defendants consented to entry of final judgments that permanently enjoin Bittrex and Shihara from violating Sections 5, 15(a), and 17A of the Exchange Act and enjoin Bittrex Global from violating Section 5 of the same Act.[71] Bittrex and Bittrex Global agreed to pay disgorgement of $14.4 million, prejudgment interest of $4 million, and a civil penalty of $5.6 million, for a total monetary payment of $24 million.[72]

In addition to actions against issuers of digital assets and trading platforms, the SEC has brought several actions against the creators of NFTs.

NFTs

Starting in November 2017, NFTs have gained notoriety as a popular means of buying and selling digital collectibles representing tangible and intangible assets across multiple industries, including art, sports, music, fashion and gaming. Perhaps the most famous NFT is when artist Mike Winkelmann, known as Beeple, used an NFT to sell his digital art "Everydays, the First 5000 Days" for $69 million on March 11, 2021,.[73] The sale was the third-highest price paid for a piece of art by a living artist. Four days prior to Beeple's sale, an NFT of a video clip of LeBron James dunking a basketball sold for $208,000 on NBA Top Shot.[74] Jack Dorsey, the creator of Twitter, auctioned his first-ever tweet as an NFT for $2.9 million.

Though the eye-popping numbers related to these NFT auctions are attention-drawing, NFTs are not just limited to digital collectibles. One of the more exciting possibilities for NFTs lies in the creation of new markets and forms of investments whereby certain physical assets can be fractionalised and sold to multiple consumers, which could increase the worth and revenue of the underlying asset. However, as NFTs proliferate across multiple mediums and technologists develop new ways to deploy NFTs, particularly in the financial services sector, these innovators will inevitably run headfirst into regulators tasked with the challenge of protecting investors and maintaining safe, sound and efficient markets.

What are NFTs?

NFTs are not like cryptocurrencies such as Bitcoin and Ethereum, which function as the native asset of a blockchain. NFTs are created as part of a platform built on an existing blockchain (like the Ethereum blockchain) and are not fungible like other cryptocurrencies, meaning that NFTs cannot be traded or exchanged for one another without inherent diminution in value (i.e., one dollar is always worth one dollar and one Bitcoin is always equal to another Bitcoin).[75] Instead, NFTs are individually unique and use blockchain technology to establish authenticity, ownership and transferability of a unique asset. An NFT is created from digital objects that represent both tangible and intangible property, including, but not limited to, (i) artwork, (ii) videos, (iii) collectibles and antiques, (iv) video game avatars, and (v) music. When an individual purchases an NFT, the purchaser can receive exclusive ownership rights to the underlying asset as well as a digital token with unique data verifying the provenance of the underlying asset. Blockchain technology and NFTs can provide artists, athletes and celebrities with a unique opportunity to leverage their fame and talent in the digital space and monetise their wares.[76] For example, artists can create and digitise their own content and sell it directly to consumers as an NFT and, in doing so, capture most of the revenue generated from such sale.

The utility of NFTs, however, can go far beyond digitising popular culture content. NFTs also carry with them the potential to revolutionise financial services, particularly investment activities among retail investors. For example, NFTs can be used to fractionalise certain assets, such as real estate, making the underlying real estate asset easier to divide among multiple owners. These fractionalised NFTs can then be tradeable on an appropriate exchange platform, which introduces new investment opportunities for investors to diversify their portfolios.

SEC guidance on NFTs

The SEC has not provided formal guidance on when an NFT is a security. The SEC staff have noted:

> ***[T]he main issue in analyzing a digital asset under the Howey test is whether a purchaser has a reasonable expectation of profits (or other financial returns) derived from the efforts of others***. A purchaser may expect to realize a return through participating in distributions or *through other methods of realizing appreciation on the asset*, such as selling at a gain in a secondary market.[77]

If an NFT relates to an existing asset and is marketed as a collectible with a public assurance of authenticity on the blockchain, it should not be deemed a security. If an NFT promises a return on investment from the efforts of others, the NFT should be deemed a security. However, as noted by the SEC staff in their 2019 Framework, "*[p]rice appreciation resulting solely from external market forces* (such as general inflationary trends or the economy) impacting the supply and demand for an underlying asset generally is not considered 'profit' under the Howey test".[78]

SEC NFT enforcement actions against issuers of NFTs

The SEC has entered into settlements with several creators of NFTs. While each case is fact-specific, the settlements shed light on the SEC's views on when an NFT will be deemed a security.

Stoner Cats

The SEC charged Stoner Cats 2 LLC ("**Stoner Cats**") with conducting an unregistered offering of crypto asset securities in the form of NFTs that raised approximately $8 million from investors to finance an animated web series called Stoner Cats.[79] According to the SEC order, on July 27, 2021, Stoner Cats offered and sold to investors more than 10,000 NFTs for approximately $800 each, selling out in 35 minutes.[80] Before and after Stoner Cats NFTs were sold to the public, Stoner Cats' marketing campaign highlighted specific benefits of owning them, including the option for owners to resell their NFTs on the secondary market.[81] The Stoner Cats team emphasised its expertise as Hollywood producers, its knowledge of crypto projects, and the well-known actors involved in the web series, leading investors to expect profits because a successful web series could cause the resale value of the Stoner Cats NFTs in the secondary market to rise.[82] The company configured the Stoner Cats NFTs to provide a 2.5 per cent royalty for each secondary market transaction in the NFTs and encouraged individuals to buy and sell the NFTs, leading purchasers to spend more than $20 million in at least 10,000 transactions.[83] According to the SEC order, Stoner Cats violated the Securities Act by offering and selling these crypto asset securities to the public in an unregistered offering that was not exempt from registration.[84] Stoner Cats agreed to a cease-and-desist order and to pay a civil penalty of $1 million.[85] The order establishes a Fair Fund to return monies that injured investors paid to purchase the NFTs.[86] Stoner Cats also agreed to destroy all NFTs in its possession or control and publish notice of the order on its website and social media channels.[87]

Impact Theory

The SEC charged Impact Theory LLC ("**Impact Theory**"), a media and entertainment company headquartered in Los Angeles, with conducting an unregistered offering of crypto asset securities in the form of purported NFTs.[88] The company raised approximately $30 million from hundreds of investors, including investors across the United States, through the offering.[89] From October to December 2021, Impact Theory offered and sold three tiers of NFTs, known as Founder's Keys, which Impact Theory called "Legendary", "Heroic", and "Relentless".[90] The company encouraged potential investors to view the purchase of a Founder's Key as an investment into the business, stating that investors would profit from their purchases if Impact Theory was successful in its efforts.[91] The company emphasised that it was "trying to build the next Disney", and, if successful, it would deliver "tremendous

value" to Founder's Key purchasers.[92] The NFTs offered and sold to investors were deemed by the SEC to be investment contracts and therefore securities.[93] Accordingly, Impact Theory violated the federal securities laws by offering and selling these crypto asset securities to the public in an unregistered offering that was not otherwise exempt from registration.[94]

Impact Theory agreed to a cease-and-desist order finding that it violated registration provisions of the Securities Act and ordering it to pay a combined total of more than $6.1 million in disgorgement, prejudgment interest, and a civil penalty.[95] The order also establishes a Fair Fund to return monies that injured investors paid to purchase the NFTs.[96] Impact Theory agreed to destroy all Founder's Keys in its possession or control, publish notice of the order on its websites and social media channels, and eliminate any royalty that Impact Theory might otherwise receive from future secondary market transactions involving the Founder's Keys.[97]

Regulation of NFT platforms

If an NFT is a security, the platform facilitating the sale and secondary trading of the NFT may have to register with the SEC as an exchange. As the SEC noted in the DAO Report, a system that meets the definition of an exchange and is not excluded under Rule 3b-16(b) must register as a national securities exchange or operate pursuant to an appropriate exemption.[98] One frequently used exemption is to register as an ATS. Rule 3a1-1(a)(2) exempts from the definition of "exchange" under Section 3(a)(1) an ATS that complies with Regulation ATS. If an NFT is a security, any platform that brings together multiple buyers and sellers of the NFT using non-discretionary methods will likely be deemed an exchange.

In addition to actions against the issuers of digital assets and stablecoins, and the creators of NFTs, the SEC has also noted that stablecoins may be securities depending on the facts and circumstances.

Staking

In September 2020, the staff of the SEC's Strategic Hub for Innovation and Financial Technology (the "**FinHub**") issued a statement in response to the Office of the Comptroller of the Currency's Interpretive Letter 1172, noting that stablecoin reserves could constitute securities and subject issuers of such stablecoins to registration, reporting and other requirements under the federal securities laws.[99] The FinHub did not provide guidance pertaining to the circumstances where a stablecoin would constitute a security. The FinHub stated that whether a stablecoin reserve constituted a security was an "inherently facts and circumstances determination ... [requiring] a careful analysis of the nature of the instrument, including the rights it purports to convey, and how it is offered and sold". The FinHub encouraged stablecoin issuers to contact them with any questions to help ensure that such stablecoins are structured, marketed and operated in compliance with the federal securities laws. The FinHub's statement notes that the FinHub staff are prepared to engage with market participants and, depending on the specific facts and circumstances, consider providing a "no-action" position regarding whether activities with respect to a specific stablecoin may involve the application of the federal securities laws.

On April 4, 2022, SEC Chairman Gary Gensler, speaking at the Penn Law Capital Markets Association Annual Conference, raised three policy concerns related to stablecoins.[100] First, Gensler noted that stablecoins raise public policy considerations regarding financial stability and monetary policy underlying SEC regulations related to money market funds and other securities. These considerations include how a stablecoin is backed and the effect that the loss of a peg or the failure of an issuer could have on the wider crypto ecosystem. Second, Gensler noted that stablecoins raise issues related to their potential use for illicit activity.

Specifically, Gensler expressed his concern with a stablecoin's ability to facilitate those seeking to sidestep public policy goals connected to the traditional banking and financial system, such as anti-money laundering, tax compliance and sanctions. Third, Gensler noted concerns related to investor protection that could benefit from greater oversight. Gensler expressed his concern with potential conflicts of interest and market integrity questions raised by stablecoins owned by crypto trading and lending platforms where customers have a counterparty relationship with the platform. Although Gensler's views are his own and do not constitute formal SEC guidance or rulemaking, Gensler's comments provide insight on the SEC's potential concerns regarding stablecoin regulation.

Kraken

The SEC charged Payward Ventures, Inc. and Payward Trading Ltd. (both commonly known as Kraken) with failing to register the offer and sale of their crypto asset staking-as-a-service programme, whereby investors transfer crypto assets to Kraken for staking in exchange for advertised annual investment returns of as much as 21 per cent.[101] The Kraken entities agreed to immediately cease offering or selling securities through crypto asset staking services or staking programmes and pay $30 million in disgorgement, prejudgment interest, and civil penalties.[102]

According to the SEC's complaint, since 2019, Kraken has offered and sold its crypto asset "staking services" to the general public, whereby Kraken pools certain crypto assets transferred by investors and stakes them on behalf of those investors.[103] Staking is a process in which investors lock up – or "stake" – their crypto tokens with a blockchain validator with the goal of being rewarded with new tokens when their staked crypto tokens become part of the process for validating data for the blockchain.[104] When investors provide tokens to staking-as-a-service providers, they lose control of those tokens and take on risks associated with those platforms, with very little protection.[105] The complaint alleges that Kraken touts that its staking investment programme offers an easy-to-use platform and benefits that derive from Kraken's efforts on behalf of investors, including Kraken's strategies to obtain regular investment returns and payouts.[106]

In addition to ceasing the staking programme and the monetary relief, Payward Ventures, Inc. and Payward Trading Ltd, without admitting or denying the allegations in the SEC's complaint, consented to the entry of a final judgment, subject to court approval, that would permanently enjoin each of them from violating Section 5 of the Securities Act and permanently enjoin them and any entity they control from, directly or indirectly, offering or selling securities through crypto asset staking services or staking programmes.[107]

Conclusion

Almost all sides recognise the potential benefits of blockchain technology and its potential and actual impact on developing innovative financial products and democratising financial services. However, the regulatory treatment of digital assets will be the primary driver as to how the technology can and will be utilised in the United States. As discussed in this chapter, a legal determination that a digital asset is a security carries significant consequences as to how the digital asset can be marketed, bought, sold, and used; meanwhile, the absence of clear regulation or legislation will only lead to an ongoing chilling effect in the United States regarding digital assets and, as a result, leave the United States behind as other jurisdictions race to develop legal frameworks to embrace and foster the use of blockchain technology and digital assets. As a result, observing this balancing act, and its evolution, among legislators, regulators, and even the judiciary, will only lead to more interesting times.

Endnotes

1. Levin, R., *et al*., "Real Regulation of Virtual Currencies" (*Handbook of Digital Currency*, 328–31 (2015)). *See also* Statement on Digital Asset Securities Issuance and Trading, Division of Corporation Finance, Division of Investment Management, and Division of Trading and Markets, SEC (Nov. 16, 2018), *available at:* https://www.sec.gov/news/public-statement/digitalasset-securites-issuuance-and-trading; https://www.gemini.com/cryptopedia/cryptocurrencies-vs-tokens-difference#section-what-is-a-digital-asset (last visited June 28, 2021); Richard B. Levin, *et al*., "Untying the Gordian Knot: custody of digital assets", 198 (2021).
2. *See id.* at 331–32.
3. PricewaterhouseCoopers, 2016, What is the blockchain?, *available at:* https://www.pwc.com/gr/en/publications/assets/qa-what-is-blockchain.pdf (last visited July 17, 2020).
4. Goldman Sachs, Emerging Theme Radar: What if I Told You... (2015), *available at:* https://www.goldmansachs.com/insights/pages/macroeconomic-insights-folder/what-if-i-told-you/report.pdf#:~:text=Emerging%20Theme%20Radar%20What%20if%20I%20Told%20You%E2%80%A6,to%20creating%20a%20alternative%20to%20fossil%20fuel%20in (last visited July 17, 2020).
5. Pinna, A., "Distributed ledger technologies in securities post-trading", European Central Bank (April 2016), *available at:* https://www.ecb.europa.eu/pub/pdf/scpops/ecbop172.en.pdf
6. *Id.*
7. Real Regulation of Virtual Currencies, *Handbook of Digital Currency* (2015).
8. *Id.*
9. *Id.*
10. Levin, R. and Tran, K., "It's the End of the World as We Know It (And I feel fine)", Lexology (Aug. 13, 2021), *available at:* https://www.lexology.com/library/detail.aspx?g=dd8fa2cb-439b-447e-9eed-07a16cdefa4d
11. Report of Investigation Pursuant to Section 21(a) of the Securities Exchange Act of 1934: The DAO (July 25, 2017) (the "**DAO Report**"), *available at:* https://www.sec.gov/litigation/investreport/34-81207.pdf
12. *Id.*
13. Clayton, J., "Statement on Cryptocurrencies and Initial Coin Offerings", SEC Public Statement (Dec. 11, 2017), *available at:* https://www.sec.gov/news/public-statement/statement-clayton-2017-12-11
14. Pound, J., "SEC Chairman Gary Gensler says More Investor Protections are Needed for Bitcoin and Crypto Markets" (CNBC, May 7, 2021), *available at:* https://www.cnbc.com/2021/05/07/sec-chairman-gary-gensler-says-more-investor-protections-are-needed-for-bitcoin-and-crypto-markets.html
15. Prentice, C. and Schroeder, P., "Analysis: Biden's SEC chair nominee signals more regulation for cryptocurrencies", Reuters (March 2021), *available at:* https://www.reuters.com/article/us-usa-crypto-currency-gensler-analysis-idUSKCN2AV02H
16. *See Reves v. Ernst & Young*, 494 U.S. 56 (1990); *see also SEC v. Edwards*, 540 U.S. 389 (2004).
17. Levin, R., Waltz, P. and LaCount, H., Betting Blockchain Will Change Everything – SEC and CFTC Regulation of Blockchain Technology, *Handbook of Blockchain, Digital Finance, and Inclusion*, Volume II (2016).
18. *Id.* The definitions of security under the Securities Act, the Exchange Act, the Investment Advisers Act of 1940 (the "**Advisers Act**"), and the Investment Company Act of 1940, do not include currencies.

19. *SEC v. W.J. Howey Co.*, 328 U.S. 293 (1946).
20. SEC Chairman Jay Clayton, Testimony on Virtual Currencies: The Roles of the SEC and CFTC, Before the Committee on Banking, Housing, and Urban Affairs, United States Senate (Feb. 6, 2018) (stating: "[B]y and large, the structures of ICOs that I have seen involve the offer and sale of securities and directly implicate the securities registration requirements and other investor protection provisions of our federal securities laws."), *available at:* https://www.sec.gov/news/testimony/testimony-virtual-currencies-oversight-role-us-securities-and-exchange-commission (last visited Sep. 23, 2020). The Chairman also stated in response to questions from a Senator at the same hearing, "I believe every ICO I've seen is a security". *Id.*
21. Section 2(a)(1) of the Securities Act of 1933 (emphasis added).
22. *See Tcherepnin v. Knight*, 389 U.S. 332 (1967); *SEC v. W.J. Howey Co*., 328 U.S. 293 (1946); *Reves*, 494 U.S. 56.
23. *See*, *e.g.*, *SEC v. FLiK, et al.* (Sep. 10, 2020), *available at:* https://www.sec.gov/litigation/complaints/2020/comp-pr2020-207.pdf; *In the Matter of Boon.Tech, et al.* (Aug. 13, 2020), *available at:* https://www.sec.gov/litigation/admin/2020/33-10817.pdf; *SEC v. ICOBox, et al*. (Sep. 18, 2019), *available at*: https://www.sec.gov/litigation/complaints/2019/comp-pr2019-181.pdf; *SEC v. Kik Interactive, Inc.* (June 4, 2019), *available at*: https://www.sec.gov/litigation/complaints/2019/comp-pr2019-87.pdf; *In the Matter of Gladius Network LLC* (Feb. 20, 2019), *available at:* https://www.sec.gov/litigation/admin/2019/33-10608.pdf; *In the Matter of Floyd Mayweather, Jr.* (Nov. 29, 2018), *available at:* https://www.sec.gov/litigation/admin/2018/33-10578.pdf; *In the Matter of Khaled* ("**DJ Khaled**") (Nov. 29, 2018), *available at:* https://www.sec.gov/litigation/admin/2018/33-10579.pdf; *In the Matter of Paragon Coin, Inc*. (Nov. 16, 2018), *available at:* https://www.sec.gov/litigation/admin/2018/33-10574.pdf; *In the Matter of CarrierEQ, Inc., D/B/A Airfox* (Nov. 16, 2019), *available at:* https://www.sec.gov/litigation/admin/2018/33-10575.pdf; *In the Matter of Zachary Coburn* (Nov. 8, 2018), *available at:* https://www.sec.gov/litigation/admin/2018/34-84553.pdf; *SEC v. Blockvest LLC, et al*. (Oct. 11, 2018), *available at:* https://www.sec.gov/litigation/complaints/2018/comp-pr2018-232.pdf; *TokenLot LLC, Lenny Kugel, and Eli Lewitt* (Sep. 11, 2018), *available at:* https://www.sec.gov/litigation/admin/2018/33-10543.pdf; *In the Matter of Tomahawk Exploration LLC and David T. Laurance* (Aug. 14, 2018), *available at:* https://www.sec.gov/litigation/admin/2018/33-10530.pdf; *SEC v. Titanium Blockchain Infrastructure Services, Inc., et al*. (May 22, 2018), *available at:* https://www.sec.gov/litigation/complaints/2018/comp-pr2018-94.pdf; *SEC v. Sharma, et al*. (April 2, 2018), *available at:* https://www.sec.gov/litigation/complaints/2018/comp-pr2018-53.pdf; *In the Matter of Munchee, Inc.* (Dec. 11, 2017), *available at*: https://www.sec.gov/litigation/admin/2017/33-10445.pdf; *SEC v. REcoin Group Foundation LLC, et al*. (Sep. 29, 2017), *available at*: https://www.sec.gov/litigation/complaints/2017/comp-pr2017-185.pdf
24. *Int'l Bhd. Teamsters v. Daniel*, 439 U.S. 551, 559 (1979). An investment of money need not be in traditional currency. *See*, *e.g.*, *SEC v. Shavers*, 2013 U.S. Dist. LEXIS 110018 (E.D. Tex. Aug. 6, 2013) (finding that making investments denominated in Bitcoin, a form of digital virtual currency, constituted an investment of money subject to federal securities laws); *see also SEC v. Shavers*, No. 4:13-CV-416 (E.D. Tex. Aug. 26, 2014) (upholding on rehearing).
25. Framework for "Investment Contract" Analysis of Digital Assets, Division of Corporation Finance, SEC (April 3, 2019), *available at:* https://www.sec.gov/corpfin/framework-investment-contract-analysis-digital-assets (last visited July 17, 2022).

26. *United Hous. Found., Inc. v. Forman*, 421 U.S. 837, 852, *reh'g denied*, 423 U.S. 884 (1975).
27. *SEC v. Edwards*, 540 U.S. 389, 394 (2004).
28. *W.J. Howey Co.*, 328 U.S. at 300.
29. *Id.* (finding that the investors had no desire to occupy the land or to develop it themselves, and they were attracted solely by the prospects of a return on their investment; if the purchasers wanted to occupy the land or to develop it themselves, the securities laws would not apply).
30. Framework for "Investment Contract" Analysis of Digital Assets (2019), *available at:* https://www.sec.gov/corpfin/framework-investment-contract-analysis-digital-assets#_edn1
31. *SEC v. Ripple Labs, Inc.*, 2023 WL 4507900 (S.D.N.Y. July 13, 2023), *available at:* https://www.nysd.uscourts.gov/sites/default/files/2023-07/SEC%20vs%20Ripple%207-13-23.pdf
32. Complaint, *SEC v. Ripple Labs, Inc.*, No. 20-cv-10832 (S.D.N.Y. Dec. 22, 2020), ECF. No. 4.
33. Newmyer, T., "SEC's Gensler likens stablecoins to 'pokerchips' amid call for tougher crypto regulation", *Washington Post* (Sep.21,2021), *available at:* https://www.washingtonpost.com/business/2021/09/21/sec-gensler-crypto-stablecoins
34. *See* Presidential Working Group on Financial Markets, Report on Stablecoins (Nov. 2021), *available at:* https://home.treasury.gov/system/files/136/StableCoinReport_Nov1_508.pdf
35. *Id.*
36. CoinMarketCap, Top Stablecoin Tokens by Market Capitalization, *available at:* https://coinmarketcap.com/view/stablecoin (last visited Oct. 18, 2023).
37. Opinion & Order, *SEC v. Terraform Labs Pte. Ltd.*, No. 1:23-cv-01346 at 40 (S.D.N.Y. July 31, 2023) Dkt. 51. ("**Terraform Order**").
38. *Id.*
39. *Id.* at 34.
40. *Id.* at 36–37.
41. *Id.*
42. 15 U.S.C. § 78c(a)(1).
43. DAO Report.
44. Regulation ATS, Rule 300(a).
45. Securities and Exchange Commission Study on Investment Advisers and Broker-Dealers (Jan. 2011), *available at:* https://www.sec.gov/news/studies/2011/913studyfinal.pdf
46. *See* Betting Blockchain.
47. *Mass. Fin. Servs., Inc. v. Sec. Investor Prot. Corp.*, 411 F. Supp. 411, 415 (D. Mass. 1977), *aff'd*, 545 F.2d 754.
48. Levin, R., *et al*., "Betting Blockchain"; *see also In re BTC Trading, Corp.*, SEC Release No. 34-73783, 2014, *available at:* https://www.sec.gov/litigation/admin/2014/33-9685.pdf
49. Securities Exchange Act Release No. 68080 (Oct. 22, 2012), 77 Fed. Reg. 66219 (Nov. 2, 2012) ("**Clearing Agency Standards**"), *available at:* https://www.federalregister.gov/documents/2012/11/02/2012-26407/clearing-agency-standards
50. *See* S. Rep. 94-75, 94th Cong., 1st Sess. 7 (1975) (the "**Senate Report**").
51. Clearing Agency Standards.
52. *Id.*

53. *In re BTC Trading, Corp.*, SEC Release No. 34-73783, 2014 ("**BTC Trading Corp.**"), *available at:* https://www.sec.gov/litigation/admin/2014/33-9685.pdf
54. Securities Exchange Act Release No. 76743 (Dec. 22, 2015), 80 Fed. Reg. 81948 (Dec. 31, 2015) ("**Transfer Agent Release**"), *available at:* https://www.sec.gov/rules/concept/2015/34-76743.pdf
55. *Id.*
56. *Id.*
57. *Id.*
58. SEC Press Release, "*SEC Files 13 Charges Against Binance Entities and Founder Changpeng Zhao*" (June 5, 2023), *available at:* https://www.sec.gov/news/press-release/2023-101#:~:text=The%20SEC's%20complaint%20alleges%20that,should%20have%20registered%20as%20a
59. Complaint, *SEC v. Binance Holdings Ltd.*, No. 23-cv-01599 (D.D.C. June 5, 2023), *available at:* https://www.sec.gov/files/litigation/complaints/2023/comp-pr2023-101.pdf
60. *Id.*
61. *Id.*
62. *Id.*
63. SEC Press Release, "*SEC Charges Coinbase for Operating as an Unregistered Securities Exchange, Broker, and Clearing Agency*" (June 6, 2023), *available at:* https://www.sec.gov/news/press-release/2023-102
64. *Id.*
65. Complaint, *SEC v. Coinbase, Inc.*, No. 23-cv-04738 (S.D.N.Y. June 6, 2023).
66. *Id.*
67. *See id.*; *see also* https://www.coinmarketcap.com (as of July 17, 2023).
68. SEC Press Release, "Crypto Asset Trading Platform Bittrex and Former CEO to Settle SEC Charges for Operating an Unregistered Exchange, Broker, and Clearing Agency" (Aug. 10, 2023), *available at:* https://www.sec.gov/news/press-release/2023-150; *see also SEC v. Bittrex, Inc., Bittrex Global GmbH, and William Shihara*, No. 23-cv-580 (W.D.W.A. April 17, 2023), *available at:* https://www.sec.gov/files/litigation/complaints/2023/comp-pr2023-78.pdf
69. *Id.*
70. *Id.*
71. *Id.*
72. *Id.*
73. Leech, Ollie, "*What are NFTs and How do they Work?*" (CoinDesk, March 23, 2021), *available at:* https://www.coindesk.com/what-are-nfts (last visited June 28, 2021); *see also* Reyburn, Scott, "*JPG File Sells for $69 Million, as 'NFT Mania' Gathers Pace*" (*New York Times*, March 11, 2021), *available at:* https://www.nytimes.com/2021/03/11/arts/design/nft-auction-christies-beeple.html (last visited June 28, 2021).
74. NBA Top Shot is a blockchain-based platform that allows customers to buy, sell and trade numbered versions of specific, officially licensed video highlights of professional basketball players.
75. Conti R. and Schmidt, J., "*What You Need to Know about Non-Fungible Tokens (NFTs)*" (*Forbes*, May 14, 2021), *available at:* https://www.forbes.com/advisor/investing/nft-non-fungible-token (last visited June 28, 2021).
76. *Id.*
77. Framework for "Investment Contract" Analysis of Digital Assets (2019), *available at:* https://www.sec.gov/corpfin/framework-investment-contract-analysis-digital-assets#_edn1

78. *Id.*
79. SEC Press Release, "SEC Charges Creator of Stoner Cats Web Series for Unregistered Offering of NFTs" (Sep. 13, 2023), *available at:* https://www.sec.gov/news/press-release/2023-178?utm_medium=email&utm_source=govdelivery; *see also In the Matter of Stoner Cats 2 LLC*, SEC Release No. 33-11233, 2023, *available at:* https://www.sec.gov/files/litigation/admin/2023/33-11233.pdf
80. *Id.*
81. *Id.*
82. *Id.*
83. *Id.*
84. *Id.*
85. *Id.*
86. *Id.*
87. *Id.*
88. SEC Press Release, "SEC Charges LA-Based Media and Entertainment Co. Impact Theory for Unregistered Offering of NFTs" (Aug. 28, 2023), *available at:* https://www.sec.gov/news/press-release/2023-163; *In the Matter of Impact Theory, LLC*, SEC Release No. 33-11226 (Aug. 28, 2023), *available at:* https://www.sec.gov/files/litigation/admin/2023/33-11226.pdf
89. *Id.*
90. *Id.*
91. *Id.*
92. *Id.*
93. *Id.*
94. *Id.*
95. *Id.*
96. *Id.*
97. *Id.*
98. DAO Report.
99. Securities and Exchange Commission, SEC FinHub Staff Statement on OCC Interpretation (Sep. 21, 2020), *available at:* https://www.sec.gov/news/public-statement/sec-finhub-statement-occ-interpretation
100. Securities and Exchange Commission, Prepared Remarks of Gary Gensler on Crypto Markets Penn Law Capital Markets Association Annual Conference (April 4, 2022), *available at:* https://www.sec.gov/news/speech/gensler-remarks-crypto-markets-040422
101. SEC Press Release, "Kraken to Discontinue Unregistered Offer and Sale of Crypto Asset Staking-As-A-Service Program and Pay $30 Million to Settle SEC Charges" (Feb. 9, 2023), *available at:* https://www.sec.gov/news/press-release/2023-25; *see also SEC v. Payward Ventures, Inc. (D/B/A Kraken) and Payward Trading Ltd. (D/B/A Kraken)*, Case No. 23-cv-588 (N.D.C.A. Feb. 9, 2023), *available at:* https://www.sec.gov/files/litigation/complaints/2023/comp-pr2023-25.pdf
102. *Id.*
103. *Id.*
104. *Id.*
105. *Id.*
106. *Id.*
107. *Id.*

Richard B. Levin
Tel: +1 303 583 9929 / Email: richard.levin@nelsonmullins.com

Richard is chair of the FinTech and Regulation Practice and was one of the first lawyers to focus on the regulation of blockchain and digital assets. He is considered a thought leader in the FinTech space. Richard brings his experience as a senior legal and compliance officer on Wall Street and in London to bear in advising clients on corporate, FinTech, securities, and regulatory issues. A problem-solver by nature, he has been advising FinTech clients on legal and regulatory issues since the start of electronic trading in the late 1990s. His practice focuses on helping financial services and technology clients identify and address regulatory issues as they build their businesses. Richard has been identified by *Chambers and Partners* as one of the leading lawyers in the Blockchain and Cryptocurrencies category since the inception of the category. He has been recognised by *Chambers* for his knowledge on regulatory matters, great relationships with regulators, for helping clients push the boundaries of the FinTech sector, and for his advice on matters such as broker-dealer licensing and alternative trading systems.

Kevin R. Tran
Tel: +1 615 664 5322 / Email: kevin.tran@nelsonmullins.com

Kevin assists clients in matters related to financial regulatory, FinTech, corporate and securities issues. He gained experience at the Federal Reserve Board in Washington, D.C., where he was a Financial Policy Analyst in the Capital and Regulatory Policy group in the Division of Supervision and Regulation. He also served the Board as the Policy Staff Adviser/Chief of Staff to the Deputy Director for Policy. In these roles, Kevin focused on developing regulations and guidance affecting banks and bank holding companies of all sizes, assisting the director with the day-to-day operations of the policy groups, and helping financial institutions and industry trade groups with regulatory interpretations.

Bobby Wenner
Tel: +1 303 583 9907 / Email: bobby.wenner@nelsonmullins.com

Bobby counsels financial services and technology firms on financial services regulatory and corporate matters. His representation is focused on financial technology companies working with blockchain, tokenization, digital assets, and cryptocurrencies, including broker-dealers, alternative trading systems (ATS), digital asset and currency trading platforms, digital asset issuers and custodians, securities exchanges, and derivatives trading platforms including swap execution facilities. Bobby represents clients before Congress, the Securities and Exchange Commission (SEC), the Financial Industry Regulatory Authority (FINRA), the Commodity Futures Trading Commission (CFTC), and state financial services regulators. He also represents banks, money services businesses, and payment proces-sors before the federal banking regulators, including the Office of the Comptroller of the Currency, the Financial Crimes Enforcement Network (FinCEN), and state banking regulators.

Nelson Mullins Riley & Scarborough LLP

MiCAR and *Morrison*: Navigating opportunities and challenges for U.S. digital asset companies in the EU and in the UK

Matthew C. Solomon, Laura Prosperetti,
Bernardo Massella Ducci Teri & Andreas Wildner
Cleary Gottlieb Steen & Hamilton LLP

Exploring opportunities and challenges in the EU under MiCAR and in the UK

With the challenging regulatory landscape in the United States prompting a quest for clearer rules, digital asset market players may look for opportunities arising from the EU's latest move. Introducing a dedicated regulatory framework for crypto-assets, Regulation (EU) 2023/1114, commonly known as "MiCAR", has emerged as a source of regulatory clarity. Enacted on June 29, 2023, MiCAR is set to roll out in phases, with partial application beginning from June 30, 2024, and further aspects taking effect from December 30, 2024.

The UK is at an earlier stage in developing its regulatory framework. Yet, the emerging future regulatory framework has already attracted interest from international firms, who are drawn to the ostensibly pro-crypto stance of the government.

This chapter focuses on MiCAR and aims to shed light on the regulatory regime that global digital asset service providers may encounter once MiCAR becomes applicable, exploring both the opportunities and the challenges that lie ahead. A precis of the evolving landscape in the UK is also provided by way of comparison.

MiCAR: Balancing crypto-asset market growth with robust supervision

The adoption of MiCAR in the EU marks a significant step towards creating financial services regulations that are fit for the digital age and contribute to a future-proof economy. MiCAR is driven by the premise that crypto-assets have the potential to bring significant benefits to market participants, such as streamlining capital-raising processes and providing faster, more cost-effective and efficient payment options.

The existing regulatory landscape for crypto-assets in the EU has considerable gaps. Until MiCAR becomes fully applicable, only crypto-assets that qualify as financial instruments under MiFID[1] and those that qualify as electronic money (e-money) under the Electronic Money Directive[2] are subject to regulation, and virtual asset service providers (VASPs) are required to comply only with anti-money laundering and counter-terrorist financing obligations.[3]

The EU's intervention is aimed at establishing a regulatory framework governing the provision of services related to crypto-assets, including the operation of trading platforms, with the aim of providing clear rules and preventing crypto-asset holders from being exposed to risks, in particular in fields not covered by consumer protection rules, as well as risks to market integrity.

The creation of a detailed regulatory framework dedicated to crypto-assets is expected to result in an increase of user confidence, significantly contributing to the development of a market in these assets, as well as in the promotion of the financial stability and smooth

operation of payment systems. At the same time, in accordance with the principle "same activity, same risk, same regulation", MiCAR establishes a full-fledged prudential framework for crypto-asset service providers (CASPs) and issuers of asset-referenced tokens (ARTs), comprising stringent authorisation, conduct of business and organisational requirements, complemented by robust supervisory powers of competent authorities.

The EU's chosen approach in adopting MiCAR reflects the significance of its goals. As a regulation, MiCAR is binding and directly applicable in all EU Member States, ensuring maximum harmonisation. This choice avoids regulatory fragmentation, safeguarding against competition distortion within the internal market. Additionally, it facilitates cross-border expansion for CASPs throughout the EU and mitigates the potential for regulatory arbitrage.

What does MiCAR entail?

In a nutshell, MiCAR establishes rules governing the issuance, public offering, and trading of crypto-assets, as well as the authorisation and supervision of CASPs, issuers of ARTs and issuers of e-money tokens (EMTs). It also provides protection for crypto-asset holders and clients of CASPs, and addresses the prevention of market abuse associated with crypto-assets.[4]

MiCAR defines crypto-assets as "*digital representation of a value or of a right that is able to be transferred and stored electronically using distributed ledger technology or similar technology*". The following categories of crypto-assets are addressed by MiCAR:

- EMTs, *i.e.*, crypto-assets that purport to maintain a stable value by referencing the value of one official currency;
- ARTs, *i.e.*, crypto-assets that are not EMTs and that purport to maintain a stable value by referencing another value or right or a combination thereof, including one or more official currencies; and
- crypto-assets other than ARTs and EMTs, which include utility tokens, *i.e.*, crypto-assets that are only intended to provide access to a good or service supplied by its issuer.

Conversely, MiCAR does not apply to crypto-assets that are: (i) unique and not fungible with other crypto-assets (NFTs) (*e.g.*, digital art and collectibles); (ii) financial instruments; (iii) deposits, including structured deposits; (iv) funds, except if they qualify as EMTs; (v) securitisation positions; (vi) non-life or life insurance products; or (vii) pension products, occupational pension schemes, individual pension products, social security schemes and similar products.

Notably, MiCAR does not currently regulate decentralised finance (DeFi) or the lending and borrowing of crypto-assets. These activities will thus remain subject to each Member State's regulation (if any) with no passporting procedure being available, possibly leading to fragmentation, an unlevel playing field, and uncertainty in the EU for market operators.

However, as part of MiCAR's periodic review, the EU Commission may make legislative proposals for the regulation of those aspects.[5]

Offer to the public and admission to trading of crypto-assets

Disclosure requirements

An offer to the public of crypto-assets and admission to trading requires the offerors to draw up, notify to the competent authority and publish an information document containing mandatory disclosures, called a crypto-asset white paper.[6] The concept of a white paper is derived from the EU's prospectus regime together with the liability regime for information contained in the white paper that is not complete, fair or clear or that is misleading. MiCAR also sets forth specific requirements for marketing communications.[7]

Conduct of business and organisational requirements

Offerors of crypto-assets other than ARTs or EMTs must have effective arrangements in place to monitor and safeguard the funds or other crypto-assets raised during their offer to the public and must identify, prevent, manage and disclose conflicts of interest. In order to further ensure protection of retail holders of crypto-assets, the latter are provided with a right of withdrawal during a period of 14 days after the relevant acquisition.

More stringent conduct of business and organisational requirements are provided for issuers of ARTs and EMTs. In particular, issuers of ARTs (other than EU credit institutions) must be authorised by the competent EU authorities of their home Member State. These authorities are also responsible for approving the crypto-asset white paper.

Issuers of ARTs must comply with various requirements, including transparent complaints-handling procedures, conflicts of interest policies, robust governance arrangements, the maintenance of own funds above certain minimum thresholds, and the adoption of a recovery plan and a redemption plan. They must also establish a reserve of assets meeting specific criteria to cover the risks associated with the assets referenced by the ARTs, and must offer ART holders the option of redeeming them at any time in the form of either funds in an amount equal to the market value of the referenced assets or delivery of the referenced assets. Moreover, the acquisition of a qualifying holding in ART issuers is subject to authorisation, involving an assessment by competent authorities of the reputation and financial soundness of the proposed acquirer.

Finally, firms wishing to issue and offer EMTs in the EU will have to be EU-authorised credit institutions or e-money institutions (or payment institutions, once the very recent EU Commission proposal is approved and enters into force),[8] subject to comprehensive prudential requirements under those frameworks. EMTs will be subject to EU regulations applicable to e-money and be redeemable at par value for funds denominated in the official currency that the EMT is referencing. Issuers of EMTs are required to safeguard the funds received in exchange of EMTs, deposit at least 30 per cent thereof in separate accounts at credit institutions and invest the remaining funds in safe assets. Issuers of EMTs are also required to adopt a recovery plan and a redemption plan.

Enhanced requirements for significant ARTs and EMTs

Certain ARTs or EMTs may be classified by the European Banking Authority (EBA) as significant on the basis of certain criteria such as a large customer base, high market capitalisation and a large number/value of transactions. Issuers may opt for a voluntary classification of the EMT or the ART as a significant EMT/ART, subject to demonstrating that the token is likely to meet the relevant criteria. Significant ART and EMT issuers will be subject to certain additional requirements and enhanced supervision by the EBA and national competent authorities. In particular, they will be required to adopt liquidity management and stress testing policies, as well as remuneration policies that promote effective risk management, comply with higher capital requirements, and ensure that tokens can be held by different CASPs.

CASPs

Alongside the issuance of crypto-assets, MiCAR regulates the provision of certain crypto-asset services that are broadly equivalent to the investment services and activities regulated under MiFID but pertain to crypto-assets instead of financial instruments.[9]

Unless crypto-asset services are provided at the exclusive initiative of the client, the provision of such services in the EU requires authorisation. Only legal persons or other undertakings that have a registered office in a Member State in which they carry out substantive business

activities may be authorised as CASPs by the competent authority of their home Member State, subject to an assessment process. Once authorised, a CASP may lawfully provide its services in other Member States under the EU passporting regime.[10]

MiCAR establishes operational, organisational and prudential requirements for CASPs, as well as conduct of business requirements that are similar to those applicable to investment firms under MiFID. CASPs must act honestly, fairly, professionally and in the best interests of their clients. To ensure consumer protection, CASPs are subject to minimum capital requirements, robust corporate governance arrangements and stringent organisational requirements. These include measures to identify, prevent, manage and disclose conflicts of interest, safeguarding clients' crypto-assets and funds, handling complaints and complying with outsourcing requirements. MiCAR also establishes a framework for the assessment and authorisation of acquisitions of qualifying holdings in CASPs, requiring, *inter alia*, that shareholders and proposed acquirers be of sufficiently good repute.

Enforcement

National competent authorities have broad supervisory and investigative powers to oversee and enforce compliance with MiCAR by issuers and offerors of crypto-assets, as well as CASPs. Those powers include the ability to request information, carry out investigations, suspend activities for suspected infringements and impose prohibitions. Competent authorities also have the power to impose significant penalties on issuers, offerors or persons seeking admission to trading of crypto-assets, and on CASPs.

In addition, with respect to issuers of significant ARTs and EMTs, the EBA has the power to supervise compliance by the relevant issuers, as well as the power to carry out on-site inspections, take supervisory measures and impose fines.

Is becoming subject to MiCAR optional?

The question of whether becoming subject to MiCAR is truly optional arises for global digital asset platforms operating from outside the EU. In practice, the answer seems to lean towards a definite "no": if offering their services in the EU, third-country CASPs will be required to obtain authorisation under MiCAR from a competent authority of a Member State and, for purposes of such authorisation, they will be required to establish a subsidiary or at least a branch in such Member State.

Similarly, third-country firms that are issuers of ARTs and intend to offer them to the public or request admission to trading in the EU will need to obtain authorisation under MiCAR, which requires an establishment in the EU, whereas issuers of EMTs will have to be legal entities established in the EU and authorised as banks or e-money institutions in a Member State.

This means that global digital asset platforms seeking to provide services in the EU will have no choice but to seek one or multiple authorisations under MiCAR and comply with the regulation. As such, the territorial scope of MiCAR casts a wide net, without room for avoidance.

What to expect from the implementation of MiCAR

The impending implementation of MiCAR in the EU comes at a time of growing scepticism towards unsound crypto models, leading to an anticipation of a highly rigorous implementation of the regulation, for which digital asset businesses should proactively prepare. A recent speech by a Member of the Executive Board of the European Central Bank (ECB) has underscored the need for robust regulatory standards and a cautious approach to public support for the crypto industry,[11] whereas the EBA has issued a statement urging financial institutions and undertakings intending to engage in ART and EMT activities

to conduct comprehensive legal and risk assessments while implementing effective risk mitigation measures. The EBA has also called upon national competent authorities to inform existing issuers of crypto-assets about the upcoming MiCAR requirements, provide consumer information, and encourage adherence to guiding principles encompassing disclosure obligations, business models assessment, and adoption of sound governance and organisational arrangements.[12]

The emerging regulatory framework in the UK

While the regulatory outcomes intended in the UK are very similar to the aims of MiCAR, there are some subtle differences, especially in the regulatory approach and proposed regulatory scope. This section will set out the key points in this respect.

What should be noted is that the centrepiece of crypto-asset service regulation is still in the early stages of its development. This means that firms, as well as other stakeholders, still have an important opportunity to voice their positions on proposed regulation and influence the future regulatory regime.

Regulation in stages

MiCAR represents a regulatory approach whereby a single piece of legislation will introduce a new, comprehensive framework for crypto-assets.

The UK's approach is markedly different. Rather than opting for a radical new scheme of regulation, the UK government adopts a staged approach to regulation, amending the current financial services regulatory framework to cover crypto-assets as well.

The UK's anti-money laundering/counter-terrorist financing regime has captured certain crypto-asset businesses (crypto-asset exchange providers and custodian wallet providers) since 2020. Now, through the Financial Services and Markets Act 2023 (FSMA 2023), the government has brought "digital settlement assets" (effectively, fiat-backed stablecoins that can be used to settle payment obligations) within the UK regulatory perimeter, with the aim that, in general, they should be regulated under e-money and payments regulation by the Financial Conduct Authority, and that systemic arrangements should also be brought within the existing framework for systemic payment systems and service providers (which are subject to Bank of England oversight).

The UK's financial promotion regime has also been amended so as to regulate the marketing of so-called "qualifying crypto-assets" (broadly, crypto-assets that are fungible and transferable) from October 2023. This is aimed at improving consumers' understanding of the risks associated with crypto-asset investments and ensuring that crypto-asset promotions are held to the same standards as broader financial services.

However, the key stages in the emergence of UK regulation are yet to come. In February this year, HM Treasury published a consultation setting out high-level proposals for the regulation of a number of crypto-asset-related services, broadly similar in scope to MiCAR, focusing on "high-priority" crypto-asset activities. HM Treasury proposes to introduce this new regulation by amending the Financial Services and Markets Act 2000 (Regulated Activities) Order 2001, which is the key legislation that establishes the perimeter of UK financial services regulation.

The government's ambition is for the UK to be home to the most open, well-regulated, and technologically advanced capital markets in the world. It believes that crypto technologies can have a profound impact across financial services and wants to capitalise on the potential benefits.

The government also envisages future phases of regulatory developments that may regulate certain crypto-asset-related activities that it does not currently consider as high priority. Examples of such activities include validation and governance activities such as mining or validating transactions, operating a node on a blockchain, or using crypto-assets to run a validator node infrastructure on a proof-of-stake network.

Like MiCAR, just a bit different

HM Treasury's proposals for the regulation of crypto-asset-related financial services are broadly similar to the framework introduced by MiCAR. That said, there are certain important nuances. At the current stage, the differences are most clearly visible in respect of the proposed regulatory scope.

In terms of the definition of crypto-assets, HM Treasury proposes to build on the definition used in FSMA 2023. FSMA 2023 defines "crypto-asset" as "any cryptographically secured digital representation of value or contractual rights that (a) can be transferred, stored or traded electronically; and (b) uses technology supporting the recording or storage of data (which may include distributed ledger technology)". Notably, unlike MiCAR, this definition does not limit crypto-assets to assets using distributed ledger technology (or "similar" technology).

More fundamental, however, is the fact that, where MiCAR imposes different levels of regulatory obligations depending on the broad category of crypto-asset (*i.e.*, EMTs, ARTs, or other crypto-assets), HM Treasury does not envisage, at least at this stage, systematic distinctions based on the category of crypto-asset in question. No ARTs, crypto-backed tokens, algorithmic stablecoins, or even NFTs would receive specific regulatory treatment based only on their characteristics. Instead, the regulatory obligations applied to market participants would depend on the specific regulated activity in question.

There are some other minor differences in the scope of MiCAR and HM Treasury's proposals in terms of the specific activities that would be regulated. For example, MiCAR imposes regulatory requirements in respect of the provision of advice on crypto-assets or portfolio management services in relation to crypto-assets. HM Treasury does not currently propose to regulate these activities. HM Treasury's consultation notes in this respect that these services are relatively limited at present and geared towards institutional and high-net-worth clients, with little immediate risk of harm to retail consumers.

On the other hand, unlike under MiCAR, HM Treasury would propose to bring lending, borrowing and leverage activities, such as operating a crypto-asset lending platform, within the regulatory perimeter. Again, this regulatory decision is risk-driven: HM Treasury highlighted in its consultation that credit risk has been a significant driver of crypto-asset market turbulence, and that, accordingly, platforms engaging in lending and borrowing activities should be required to have sufficient financial resources to manage counterparty credit risk and meet liabilities as they fall due.

Regulation in the United States

Firms looking to benefit from the comparative certainty offered by MiCAR or the UK regulatory framework may question whether they could still face private or public actions in the United States. The U.S. securities laws generally do not apply extraterritorially – either in the context of traditional securities or transactions in digital assets that could potentially be "investment contracts" and therefore securities transactions – unless specific circumstances, described below, are present. *See Morrison v. Nat'l Australia Bank Ltd*., 561 U.S. 247, 265 (2010). In 2010, the Supreme Court in *Morrison* held that the U.S. securities

laws apply only to "transactions in securities listed on domestic exchanges, [or] domestic transactions in other securities". *Id*. at 267. Applying *Morrison*, courts have held that securities transactions are domestic only where irrevocable liability was incurred or passage of title transferred in the United States. *Absolute Activist Value Master Fund Ltd. v. Ficeto*, 677 F.3d 60, 66-69 (2d Cir. 2012); *see*, *e.g.*, *Stoyas v. Toshiba Corp.*, 896 F.3d 933 (9th Cir. 2018) (adopting the *Absolute Activist* irrevocable liability test).

While *Morrison* itself was a fraud case, courts have consistently applied it to the strict liability registration provisions of the Securities Act. *See*, *e.g.*, *SEC v. Bio Def. Corp*., 2019 WL 7578525, at *11-13 (D. Mass. Sept. 6, 2019) (applying *Morrison* to Section 5 of the Securities Act); *Schentag v. Nebgen*, 2018 WL 3104092, at *5, 10-13 (S.D.N.Y. June 21, 2018) (dismissing the Section 5 claim under *Morrison*). Courts have similarly applied *Morrison* to registration provisions of the Securities Act in the context of digital asset transactions outside the United States. *See*, *e.g.*, *SEC v. Ripple Labs, Inc*., 2022 WL 762966, at *11 (S.D.N.Y. Mar. 11, 2022) (applying *Morrison* to claims under Section 5 of the Securities Act) and *Anderson v. Binance*, 2022 WL 976824, at *4 (S.D.N.Y. Mar. 31, 2022) (applying *Morrison* to claims under Section 12 of the Securities Act).

Applying *Morrison*, certain courts have held that transactions on foreign digital asset exchanges are extraterritorial, just as securities transactions on the London Stock Exchange or Euronext Paris would similarly be outside the scope of the U.S. securities laws. *See Anderson*, 2022 WL 976824, at *4 (holding that plaintiffs' transactions on a foreign cryptocurrency exchange "cannot qualify as domestic" under *Absolute Activist*, as plaintiffs needed to allege more than they "bought tokens while located in the U.S."), *appeal pending*, No. 22-972 (2d Cir.) and *Holsworth v. BProtocol Found.*, 2021 WL 706549, at *1, *3 (S.D.N.Y. Feb. 22, 2021) (dismissing the claim under *Morrison* where the plaintiff purchased digital coins on a cryptocurrency exchange located in Singapore). Whether U.S. authorities would seek to assert jurisdiction over foreign digital asset companies would be informed by what alleged conduct is at issue and the company's U.S. nexus. For the registration provisions of the U.S. securities laws, courts have held that the mere location of purchasers in the United States does not satisfy that test. *See*, *e.g.*, *Absolute Activist Value Master Fund Ltd. v. Ficeto*, 677 F.3d 60, 69 (2d Cir. 2012) ("[a] purchaser's citizenship or residency does not affect where a transaction occurs; a foreign resident can make a purchase within the United States, and a United States resident can make a purchase outside the United States") and *Anderson v. Binance*, 2022 WL 976824, at *4 (S.D.N.Y. Mar. 31, 2022) (plaintiffs' transactions on a foreign cryptocurrency exchange "cannot qualify as domestic" under *Absolute Activist*, as plaintiffs needed to allege more than they "bought tokens while located in the U.S.").

The likelihood that a court would apply the U.S. securities laws to claims against a foreign digital asset company would increase if the company allegedly engaged in fraud that was directed at or affected U.S. investors. In enforcement actions alleging fraud, the "conduct and effects" test would likely apply rather than *Morrison*'s transactional test. *See* 15 U.S.C. § 78aa; 15 U.S.C. § 77v. This test requires either: (1) "conduct within the United States that constitutes significant steps in furtherance of the violation, even if the securities transaction occurs outside the United States and involves only foreign investors"; or (2) "conduct occurring outside the United States that has a foreseeable substantial effect within the United States". *Id*. The Securities and Exchange Commission, the Commodity Futures Trading Commission, the Department of Justice, and private plaintiffs have not hesitated to bring actions against foreign digital asset companies that are alleged to have engaged in fraud.

Both U.S. authorities and private plaintiffs have taken aggressive stances with respect to foreign digital asset companies when there is alleged misconduct that has some alleged nexus to the United States. But, again, the U.S. securities laws do not apply extraterritorially, and foreign companies defending against securities claims may have sound arguments under well-settled precedent that plaintiffs have exceeded the territorial scope of these laws.

* * *

Endnotes

1. Directive 2014/65/EU of the European Parliament and of the Council of May 15, 2014 on markets in financial instruments.
2. Directive 2009/110/EC of the European Parliament and of the Council of September 16, 2009 on the taking up, pursuit and prudential supervision of the business of electronic money institutions.
3. Under the Fifth EU Anti-Money Laundering Directive, *i.e.*, Directive 2018/843/EU of the European Parliament and of the Council of May 30, 2018 amending Directive (EU) 2015/849 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing.
4. In particular, MiCAR establishes rules to prevent market abuse for crypto-assets traded, aiming to foster market confidence and integrity, with certain requirements for issuers, offerors, and persons seeking admission to trading, including treatment of inside information, public disclosure, and prohibition of insider dealing and market manipulation, while persons professionally arranging or executing transactions in crypto-assets must implement effective systems to detect manipulation.
5. The EU Commission is required to submit reports to the European Parliament and Council. These reports, including an interim report after full application of MiCAR (June 30, 2025) and another one by June 30, 2027, may be accompanied by legislative proposals to make changes to MiCAR or regulate aspects not covered by MiCAR (such as DeFi). The EU Commission must also present a report on the latest crypto-asset developments, including issues not covered by MiCAR (such as the necessity of regulating lending and borrowing of crypto-assets and NFTs), by the full application date (December 30, 2024), which may be accompanied by a legislative proposal.
6. The crypto-asset white paper must contain, *inter alia*, general information on the issuer, offeror or person seeking admission to trading, on the project to be carried out with the capital raised, on the rights and obligations attached to the crypto-assets, on the underlying technology used for such crypto-assets and on the related risks.
7. In particular, marketing communications are to be clearly identifiable as such, the information therein shall be fair, clear and not misleading and consistent with the information in the crypto-asset white paper, they shall clearly state that a crypto-asset white paper has been published and clearly indicate the address of the website and the contact details of the offeror, the person seeking admission to trading, or the operator of the trading platform for the crypto-asset concerned, and contain a statement in the form indicated under Article 7(1) MiCAR.
8. *See* the so-called PSD3 package published by the EU Commission on June 28, 2023 – comprising a Proposal for a Directive on payment services and electronic money services in the internal market (PSD3) (COM(2023) 366 final 2023/0209(COD)) and a Proposal for a Regulation on payment services in the internal market (PSR)

(COM(2023) 367 final 2023/0210(COD)) – which, among other things, provides for the merger of the regulatory regimes applicable to payment institutions and e-money institutions.

9. These include: (a) providing custody and administration of crypto-assets on behalf of clients; (b) operation of a trading platform for crypto-assets; (c) exchange of crypto-assets for funds; (d) exchange of crypto-assets for other crypto-assets; (e) execution of orders for crypto-assets on behalf of clients; (f) placing of crypto-assets; (g) reception and transmission of orders for crypto-assets on behalf of clients; (h) providing advice on crypto-assets; (i) providing portfolio management on crypto-assets; and (j) providing transfer services for crypto-assets on behalf of clients.
10. Crypto-asset services may also be provided by EU-authorised credit institutions, central securities depositories, investment firms, market operators, e-money institutions, UCITS management companies, or alternative investment fund managers, subject to advance notification requirements.
11. *See* speech by Fabio Panetta, Member of the Executive Board of the ECB, at a panel on the future of crypto at the 22nd BIS Annual Conference, June 23, 2023 (https://www.ecb.europa.eu/press/key/date/2023/html/ecb.sp230623_1~80751450e6.en.html).
12. *See* EBA statement of July 12, 2023 (https://www.eba.europa.eu/sites/default/documents/files/document_library/Publications/Other%20publications/2023/Statement%20on%20%20preparatory%20steps%20towards%20application%20of%20MiCAR/1057527/Statement%20on%20timely%20preparatory%20steps%20towards%20the%20application%20of%20MiCAR%20to%20asset-referenced%20and%20e-money%20tokens.pdf).

Matthew C. Solomon
Tel: +1 202 974 1680 / Email: msolomon@cgsh.com

Matthew C. Solomon is a partner in the Washington, D.C. office of Cleary Gottlieb. Drawing on his 15-year government career during which he held senior positions at the DOJ and SEC, Matt advises corporate, financial institution, private fund and individual clients on criminal and civil securities enforcement and litigation, general complex commercial litigation and white-collar criminal defence. He regularly practises before the DOJ, SEC, CFTC, FINRA and other domestic and foreign regulators and self-regulatory organisations, and in state and federal courts nationwide.

Before joining Cleary, Matt was the SEC's Chief Litigation Counsel, where he supervised around 120 trial lawyers nationwide.

Laura Prosperetti
Tel: +39 06 6952 2640 / Email: lprosperetti@cgsh.com

Laura Prosperetti is counsel based in the Rome office of Cleary Gottlieb. Her practice focuses on EU and Italian banking and financial law and regulation. Laura regularly advises clients on a broad range of regulatory, transactional and enforcement matters, including compliance issues linked to the implementation of EU financial regulatory reforms (in the fields of capital requirements, corporate governance, derivatives clearing, bank recovery and resolution, crypto-assets, credit ratings, investment funds, consumer credit, payment services, transparency, and anti-money laundering), mergers and acquisitions of regulated entities, and regulatory investigations and enforcement.

Bernardo Massella Ducci Teri
Tel: +39 06 6952 2290 / Email: bmassella@cgsh.com

Bernardo Massella Ducci Teri is an associate based in the Rome office of Cleary Gottlieb. His practice mainly focuses on EU and Italian banking and financial regulation, with significant experience in litigation and enforcement matters, as well as cross-border regulatory investigations and white-collar criminal proceedings relating to alleged breaches of banking and financial regulation.

Bernardo regularly advises clients on a broad range of regulatory, corporate, bankruptcy, litigation and enforcement matters (in the fields of capital requirements, corporate governance, crypto-assets, investment services, consumer credit, payment services, transparency, and anti-money laundering).

Andreas Wildner
Tel: +44 20 7614 2248 / Email: awildner@cgsh.com

Andreas Wildner is an associate based in the London office of Cleary Gottlieb. His practice encompasses a wide range of regulatory matters, with a specialisation in UK and EU financial services regulation, financial sanctions and sustainability regulation.

Andreas regularly advises clients on a broad range of regulatory issues, including in respect of securitisation and derivatives transactions, banking regulation, sustainability disclosure requirements, and the impact of sanctions on businesses operating in, or transacting with entities located in, sanctioned countries.

Cleary Gottlieb Steen & Hamilton LLP

One Liberty Plaza, New York, NY 10006, USA
Tel: +1 212 225 2000 / URL: www.clearygottlieb.com

Trends in the derivatives market and how recent fintech developments are reshaping this space

Jonathan Gilmour & Tom Purkiss
Travers Smith LLP

Some of the key developments that are currently reshaping the derivatives market are: (i) the use of smart contracts; and (ii) the implementation of digital asset referencing derivatives.

In this chapter, we cover the potential benefits that these technologies bring, some of the challenges that remain as obstacles to their widespread use, and the work that industry bodies are doing to facilitate their adoption in the market. We also briefly discuss some of the legal uncertainties and potential litigation risks arising from these developments.

Use of smart contracts

As the market continues to develop, market participants are showing ever-increasing interest in smart contracts. This interest stems from a growing body of evidence that, as detailed further below, their use in appropriate circumstances can bring with it significant efficiencies and benefits.

In response to this enthusiasm, industry bodies such as the International Swaps and Derivatives Association (**ISDA**) have been working with its market participants on the development of technology-enabled solutions (including the use of smart contracts), which will allow a fundamental reshaping of the derivatives infrastructure. ISDA's view is that these solutions should improve operating efficiency, reduce operating costs and risk, and increase both quality and transparency of data.

What is a "smart contract"?

There is no universally accepted definition for "smart contract", but this term is commonly used to refer to legal contracts (or elements of legal contracts) being represented and/or executed by software. The term "smart" refers to the fact that some elements of a smart contract are automatic and self-executing pursuant to pre-defined conditions.

The market is evolving to differentiate a "smart legal contract" from a smart contract code. A smart legal contract is a legally enforceable contract in which some or all of the contractual obligations are performed automatically by a computer program. A smart contract code, on the other hand, would not necessarily form part of a smart legal contract, but would constitute a piece of code (or programming language) designed to provide for the execution of certain tasks by a machine. The latter could indeed simply automate the performance of a natural language contract.

Potential advantages of smart contracts

- **Increased operational efficiencies** – with contracts capable of being executed immediately following the completion of a condition, delays and errors associated with the human processing of contracts and information can be avoided. Furthermore, the terms of the contract can also be automatically adjusted and updated if necessary, reducing the possibility of delay and error that would be present in a manual process.

- **Reduction in performance risk** – in a traditional contract, there is a promise to be fulfilled in the future and the risk that it may not take place. The use of automated code in a smart contract can, assuming that the code is accurate and produces its desired effect, reduce the risk of non-performance by a counterparty.
- **Reduced costs** – the elimination of intermediaries can also cut the costs they introduce into the process of actioning a contract.
- **Transparency** – if the smart contract utilises blockchain technology, the parties to a smart contract will have access to the same single source of information simultaneously, removing the possibility of deliberate or accidental manipulation of terms and discrepancies.
- **Security** – smart contracts are most often encrypted and, as above, when the smart contract is based on blockchain technology, the data becomes immutable, with anyone seeking to make changes needing to alter the entire chain to change a single record.
- **Decentralised finance (DeFi)** – as further detailed below, smart contracts could possibly be used for the issuing, servicing, trading and settling of various digital asset-based derivatives, opening up the possibility for new opportunities and innovative products in the digital asset derivatives space.

Latest developments in the derivatives market

ISDA has undertaken a significant amount of work in recent years to facilitate the use of smart contracts across the derivatives industry. This includes:

(i) The issuance of the Common Domain Model (the **CDM**), the latest version of which (ISDA CDM 2.0) was published in 2019. The CDM is a standardised solution aimed at providing market participants with a common digital representation throughout the lifecycle of a derivatives transaction. In its first two phases, the CDM provides for the representation of certain events in a machine-readable format with a focus on interest rate and credit derivatives, including an initial representation of equity swaps products and the ISDA Credit Support Annex for initial margin. It is expected that, in its next phases, the CDM will be further developed to incorporate models for foreign exchange (**FX**) transactions.

To aid the use of the CDM, ISDA published its 2021 ISDA Interest Rate Derivatives Definitions (the first to be published in a natively digital format). They were specifically drafted so that the definitions use formulae instead of legal narrative to describe concepts such as day-count fractions and interpolation so as to allow them to be more easily machine readable. The intention is also that, in time, the mechanics of the definitions will also be available via open-source code and aligned with the CDM in order to allow them to be consistently interpreted by automated systems.

(ii) Over the past few years, ISDA has published a series of papers focused on providing *Legal Guidelines for Smart Derivatives Contracts*. These papers set out ways in which derivatives contracts may be modernised and automated through the use of blockchain technology and other fintech developments, beginning with an *Introduction* to the subject in January 2019.

(iii) On 23 June 2020, ISDA launched the ISDA Clause Library, which sets out standardised drafting options for frequently negotiated provisions within the ISDA Master Agreement. The database is expected to improve the efficiency of contract negotiation and facilitate the digitisation of legal documentation. The ISDA Clause Library has since been expanded to include ISDA's collateral documentation.

(iv) On 21 January 2021, ISDA made the ISDA Master Agreement and ISDA Clause Library digitally available for the first time via ISDA Create. ISDA Create allows users to produce and agree documentation online, as well as store legal data from these documents.

(v) On 22 November 2022, ISDA launched Digital Regulatory Reporting (**DDR**) 1.0. DDR intends to support compliance with Commodity Futures Trading Commission (**CFTC**) swap data reporting rules. Using the CDM, DDR can transform interpretations of CFTC amendments into code and allows market participants to view industry interpretations of regulation.

(vi) On 26 January 2023, ISDA published new standard documentation for the trading of digital asset derivatives along with an accompanying white paper, the ISDA Digital Asset Derivatives Definitions. This has created a standard contractual framework around the ISDA Master Agreement in the hope that setting out standard provisions will aid the assessment of market risk and the contractual obligations involved, creating greater certainty for market participants.

ISDA has acknowledged the challenges in implementing the use of smart contracts (and other technology-enabled solutions) in the derivatives space and has established a number of internal committees and industry-wide working groups to focus on technology-related topics. These include the ISDA Legal Technology Working Group, the ISDA Smart Contracts/DLT Legal Working Group, the ISDA CDM Design Working Group and the ISDA Clause Library Project.

Issues and challenges to be considered from a buy-side perspective

It is promising that a number of jurisdictions have turned their attention to the interaction of smart contracts with the existing legal system. To take England and Wales as an example, the Law Commission has recently expressed its view that English law is able to facilitate and support the use of smart legal contracts without the need for any statutory reform. However, there are a number of issues and challenges that will need to be considered by ISDA in its discussions with market participants to facilitate the transition of the derivatives market towards the use of smart contract code and smart legal contracts.

Scope of automation: operational and non-operational clauses

The main payment and delivery obligations in respect of a derivatives transaction are dependent on conditional logic, so these would be well placed for being represented into a smart legal contract. However, not all clauses are susceptible to being automated and self-executed. Certain legal terms are subjective in nature and would produce ambiguity if represented in smart contract code.

The materials produced by ISDA relating to the use of smart contracts in the derivatives space suggest that when determining which parts of a derivatives contract are susceptible to automation, it is helpful to distinguish between operational and non-operational clauses. Operational clauses would generally contain conditional logic so would be more susceptible to automation, whereas non-operational clauses would more likely relate to the wider contractual relationship between the parties, proving to be more resistant to automation.

Issues with legal validation

In order to ensure that a smart legal contract produces its intended legal effect, it may be prudent for parties to obtain "legal validation" of its automated provisions (or smart contract codes) by a lawyer. However, this presents its own challenge and would require the lawyer in question to understand the programming language. It follows that there is the need for programmers to work in collaboration with lawyers to leverage their legal insight into which parts of the ISDA documentation framework would be legally effective if converted into an automatable form. ISDA is expected to play an important role in facilitating this work.

It will be challenging for non-operational clauses that include some degree of subjective interpretation (e.g. where a party is required to act in good faith or in a commercially

reasonable manner) or those that are more complex in nature (e.g. when an event of default is linked to the occurrence of a specific event outside the contractual relationship and that is not easily asserted) to be legally validated.

In addition, even if legally validated, there is a risk that the smart contract code will produce terms at the transaction confirmation level that are inconsistent with terms in the ISDA Master Agreement (or schedule). Appropriate mechanisms for resolving any consequent conflicts will need to be considered.

Issues with automation

Not all provisions, when automated, would produce the same effect as if complied with in their original form (i.e. in natural language) without automation.

By way of example, upon the occurrence of an event of default under a derivatives contract, the non-defaulting party would have the right to terminate the outstanding transactions. Under normal circumstances, under a non-automated contract, there are a range of factors that the non-defaulting party would take into account before pulling the trigger – these tend to be subjective and include commercial considerations, the relationship context at the time of the event, and the nature of the default. It would be difficult to cater for these factors when translating event of default provisions into programming language. In practice, the occurrence of an event of default under a smart legal contract would usually be self-automated, so it would automatically trigger the termination of any outstanding transactions.

ISDA has proposed to work with its members to select provisions within the ISDA documentation framework that are best suited for automation – their goal is to select provisions that can be automated without changing their legal effect.

Interaction with third-party data and platform providers

Where a smart derivatives contract involves the use of external, third-party data sources (sometimes referred to as "oracles"), there may be risks posed by data inaccuracies, whether caused by error or deliberate manipulation – particularly if hacking is involved.

For instance, smart derivatives contracts for FX derivatives will use an external data source to determine FX rates. In a situation where payment or delivery is automatically triggered by data from an external source (e.g. if automation involves any straight-through processing), the prospective apportionment of liability in the event of a third-party data failure should be considered.

In addition, consideration should be given to what alternate mechanism should be used where there is a breakdown in communication between the third party and the smart contract, due to, for example, a software programming bug or a coding error on the part of the third party. This could be with recourse to manual input.

ISDA has also identified cryptocurrency as an area of concern when considering interaction with third-party platforms. On 26 January 2023, ISDA published a white paper specifically looking at the legal risk questions that come with holding cryptocurrency in exchanges or intermediaries and, specifically, the possible issues that may cause for netting and collateral enforceability. These considerations were built upon in a further white paper published by ISDA on 3 May 2023. This white paper focuses on how digital assets held through intermediaries will be affected by the insolvency of the intermediary. ISDA identified that, from a US and English law perspective, private legal concepts such as trusts, existing insolvency regimes and rules requiring segregation of assets all act as protections for digital assets held with intermediaries. However, the white paper also highlights that issues surrounding which governing law applies and which courts have jurisdiction to enforce

claims still require significant consideration. As cryptocurrency is an area that still lacks significant regulation, these ISDA white papers offer insights to market participants to ensure that they are aware of different market risks. In this paper, ISDA suggests that development of contractual standards will be crucial in providing clarity in this area.

Complex and bespoke derivatives contracts

Certain derivatives contracts can be heavily negotiated and customised to apply to bespoke arrangements made between the parties. The level of customisation might vary depending on counterparty type and product complexity. Examples of highly customised arrangements include total return swaps, longevity swaps and other structured finance products that will likely be made under a wide set of documents forming the overall derivatives architecture where various levels of obligations apply across different parts of the documentation. It would be challenging to translate these interlinking obligations into programming language in a straightforward manner.

The recent regulatory developments in the derivatives space (which follow a global trend since the global financial crisis) have also contributed to the complexity of certain derivatives contracts; e.g. there is an increase in the use of third-party custodians when implementing collateral arrangements to deal with certain margin requirements, and there are additional layers of complexity arising from the need for certain over-the-counter derivatives transactions to be centrally cleared. Technology can provide greater clarity for these regulatory complexities and DDR is an example of this. By using code to set up a framework that makes industry interpretation of CFTC rules widely available, DDR promotes consistency as market participants are always able to refer to the same industry standard.

Laws affecting contractual performance

Certain laws might have the effect of interrupting the performance of contracts – e.g. where a provision under a specific contract is rendered void, or where a contractual stay is applied to a party in financial distress under the applicable regulatory regime. How would smart legal contracts interact with these laws? This is another issue to be considered by ISDA in its discussions with market participants.

Liquidity concerns

Once the market has moved to address most of the key concerns that are set out in this chapter, it is likely that only the largest and most sophisticated market participants will be able to start using smart legal contracts. The smaller or less sophisticated players, including many buy-side entities, might find it more challenging and costly to adapt their processes to the new "reshaped" derivatives market.

It is clear, therefore, that a number of challenges remain to be addressed before widespread use of smart contracts in the derivatives space can take hold. However, steps towards adoption are being taken. For example, at the end of 2021, Vanguard, State Street and Symbiont partnered to complete the margin calculation process for a live trade of a 30-day FX forward contract using Symbiont's distributed ledger technology (**DLT**). They have stated that they hope that this will enable the underlying FX forward contracts to be digitised and automated into a smart contract, with the expectation being that the use of smart contracts and blockchain technology could minimise counterparty risk in the FX forward currency market by around 80 per cent compared to the existing standard. Vanguard has since announced its intention to utilise DLT across its funds that utilise FX forwards throughout 2022. Trials and attempts at implementation such as this will no doubt be watched by other market participants with great interest.

Derivatives referencing digital assets

As the importance, adoption and legal recognition of digital assets has grown, naturally so too has the market for derivatives products referencing them. Bitcoin futures trading was first supported by US-regulated exchanges in December 2017, which brought with it the first influx of institutional investment in digital assets by allowing such institutional investors to obtain synthetic exposure to them and thereby avoid the need to establish custody capabilities. There are now approximately 20 futures commission merchants (**FCMs**) in the US that support listed derivatives referencing digital assets, and indeed even the most established and traditional institutions such as Goldman Sachs have started trading products tied to Bitcoin and Ethereum. Outside the US, less stringently regulated offshore digital asset derivatives exchanges have proved popular with retail investors.

The growth in the industry is undeniable, with institutional cryptocurrency funds attracting record inflows in 2021. Investment products tied to cryptoassets registered $9.3 billion in inflows during 2021 (an increase of $2.5 billion from 2020), with Bitcoin funds attracting $6.3 billion worth of this capital according to data released by CoinShares.

Despite this growth, however, the size of the market for derivatives referencing digital assets such as cryptocurrency remains dwarfed by traditional currency markets. The vast majority of this limited trading so far has been in Bitcoin and Ethereum futures and options listed on centralised exchanges such as CME, with those being far and away the most popular choices for institutional investors. Because of this focus on Bitcoin and Ethereum from the biggest players, even though there are thousands of digital asset tokens in circulation, existing derivatives reference only a fraction of these. It is, however, expected that a wider variety of products and reference assets will emerge as volumes rise and the market matures. Indeed, 37 new products were launched in 2021 and it is not unreasonable to expect that the menu of digital asset referencing products available to investors will eventually mirror traditional instruments.

Trends in the market and problems to be resolved

(1) **DeFi** – whilst traditional markets are beginning to embrace digital asset derivatives, in parallel a "shadow" financial system has been emerging that utilises blockchain technology and smart contracts to offer financial products (including digital asset derivatives) to investors. Widespread use of this technology has the potential to lower transaction costs and increase the speed of execution, introducing the possibility of it beating out more traditional offerings in the long term and leading to novel products being offered, such as DeFi options vaults.

(2) **Regulation** – generally, regulators have so far sought to fit digital assets and the derivatives that reference them within the existing legal and regulatory framework, though approaches do vary. The UK Law Commission has taken the view that digital assets fit within the existing concept of property in English law and that smart contracts operate in a sufficiently similar way to traditional contracts, such that English law is able to facilitate and support their use without reform, whilst also commenting on some of the more unique challenges they do raise. In the US, regulators have also sought to continue an approach consistent with their regulation of other derivatives and have prohibited those that cannot be squared with that framework (including those traded on less stringently regulated foreign exchanges). This has notably included the CFTC fining Kraken $1.25 million in September 2021 for failing to register as an FCM and illegally offering margined retail commodity transactions in digital assets, though consultations have been launched in an effort to better accommodate the emergence of digital assets. The EU has become one of the first to introduce a comprehensive

regulatory framework for cryptoassets with the introduction of the Markets in Crypto-Assets Regulation (**MiCA**). The aim of MiCA is to further innovation in this sector in the EU by improving investor confidence through offering them greater protection and seeking market stability. China, on the other hand, has continued to clamp down on digital assets altogether, with measures introduced by regulators extending to a prohibition on the cross-border provision of digital asset derivatives into China.

(3) **Bilateral derivatives and standardisation** – when digital asset derivatives were first traded, there was no standardised approach to documentation that could be readily used, resulting in legal negotiations acting as a significant burden on developing the market and a consequent lack of bilateral derivatives contracts. As further detailed below, however, industry bodies have now begun to turn their attention to standardisation in this space with the hope of improving transparency and liquidity. One of the most recent examples of market development is the ISDA Standard Definitions for Digital Asset Derivatives, which create a standardised approach and contractual framework for the ISDA Master Agreement. The ability to refer to standard contractual provisions not only creates greater efficiency but allows parties to better assess their contractual risk and obligations.

(4) **Valuation** – the decentralised nature of cryptocurrencies and other digital assets becomes problematic when it comes to valuation of the assets underlying the transaction, which will ultimately determine payment obligations and close-out values. Whilst equities and other securities can often be valued on the basis of a single, dominant exchange, this is not necessarily the case for a digital asset and a consensus on valuation can therefore be more difficult to reach. Issues are also presented by a lack of liquidity or manipulation impacting prices on certain exchanges. Third-party valuation services can be utilised to provide a neutral arbiter, but their discretion in valuing the assets in the absence of a clear metric can introduce its own uncertainties.

(5) **Disruption events** – there are some events that can affect digital assets that existing architecture was never intended to accommodate, e.g. forks and cyber-attacks. In the case of forks, which occur where, as a result of changes to the underlying technology or protocol, new versions of a relevant asset come into being, an entirely bespoke treatment may be required in the documentation. Additional prudence may also be required due to the volatility of the market and the enhanced risk of cyber-attack, with recent, high-profile thefts such as that which occurred at Poly Network highlighting the vulnerabilities that can be associated with the underlying asset.

ISDA

As previously stated, for a long time there was no standardised approach to documenting digital asset derivatives. Some market participants were using ISDA documentation with bespoke amendments, whilst others were using entirely bespoke documentation. This necessitated protracted negotiations between counterparties, reducing efficiency and transparency. This burden could ultimately lessen the appetite for digital asset derivatives.

In an effort to resolve this, ISDA launched a working group (the ISDA Digital Assets Legal & Documentation Group) to identify and consider the unique issues relating to digital asset derivatives, and to consider how these could best be approached and resolved prior to the introduction of market-standard definitions and documentation.

This work culminated in the publication of ISDA's Contractual Standards for Digital Asset Derivatives, in which they suggested that the use of digital assets in conjunction with smart contract code could revolutionise financial markets by improving efficiency and accuracy through automation. ISDA also identified disruption events, valuation issues and further

consideration of how digital assets could fit within the existing ISDA Master Agreement architecture as the three leading issues that needed to be resolved before standardised digital asset derivatives documentation could be produced.

ISDA has expressed a clear prioritisation of the development of legal standards to support the digital asset derivatives market in the year ahead, noting the need to facilitate greater automation, accommodate different technologies and integrate this into market infrastructure. One of ISDA's first priorities is stated to be creating documentation for cash-settled products in native digital assets such as Bitcoin. Facilitating greater automation and standardisation is evident in the ISDA Standard Definitions for Digital Asset Derivatives. The definitions have been created using a controlled language structure that can be easily translated into code and therefore integrated with the CDM and eventually fully automated as part of a smart contract. Currently, the definitions provided only cover non-deliverable forwards and options on Bitcoin and Ether but, with a flexible coding model, the hope is to expand this to other digital assets.

It should further be welcomed that ISDA's membership is expanding beyond traditional finance firms to incorporate institutions with more of a digital asset focus, with a cryptocurrency exchange joining as a member in late 2021. This should ensure that digital assets continue to receive attention and that the voice of the firms most heavily involved with them is heard across the spectrum of ISDA's work.

Legal uncertainty and potential litigation risks resulting from the above developments

Whilst developments in this space herald an exciting opportunity for market participants, it is inevitable that the introduction of new technologies and paradigm of contractual obligations and performance is likely to lead, at least initially, to legal uncertainty and therefore litigation risk. The following are some examples of issues that may arise in that context.

Conflicts between natural language and smart contract code

As noted above, the process of "legal validation" seeks to ensure as far as possible that any smart contract code accurately implements the parties' intentions. However, it may subsequently turn out that it does not do so for various reasons; for example, that the "legal validation" process was not properly carried out, or that an unexpected bug caused the software to perform in a way that could not have been expected. Whatever the reason, a dispute may arise as to what the legally operative term was, i.e. whether it was the smart contract code itself, or some other putative intention of the parties.

This uncertainty ought generally to be capable of being avoided by the expression of a clear choice by the parties as to the legal primacy of smart contract code or otherwise. One option would be for the natural language part of the contract to specify that a particular smart contract code is a mere method of performance of a particular natural language contractual term and that it is the latter that will constitute the contractual term, and not the former. The other option would be for the natural language part of the contract to specify that a piece of smart contract code shall constitute and define the relevant contractual term and that it shall have precedence over any accompanying natural language explanation or prior agreement between the parties. This has been explored by ISDA in its recent launch of new Standard Documentation and Definitions for Digital Asset Derivatives. The approach taken in this scenario has been to use a restricted form of natural language by creating a controlled language structure that can then be easily translated into code when needed.

Potential disputes are likely to arise in the absence of any such indication one way or another. This may be a more common occurrence amongst smart contracts involving non-sophisticated parties utilising DeFi where there may be no or very little natural language

contractual terms accompanying the transaction in question, as opposed to transactions involving carefully negotiated contracts between sophisticated parties.

Interpretation

It may be thought that no particular issues relating to the interpretation of smart contract code should arise: either the natural language term defines the contractual term with the smart contract code being a mere method of performance, in which case the only thing to be interpreted is the natural language term in the usual way; or the smart contract code itself defines the contractual term, in which case, whatever it does will be deemed to have been the intention of the parties. Whilst this is a very neat picture, it may not reflect reality.

First, as noted above, the interaction and relative priority between any natural language term and the relevant smart contract code may not be all that clear. Secondly, it may not necessarily be correct that, by the parties agreeing that a piece of smart contract code shall define the contractual term, they have thereby agreed to whatever the code does, even if it leads to results that were completely unforeseen and unintended by the parties, considered both subjectively and objectively. Such an interpretation *may* be possible if there are clear words to that effect, but it is questionable how many parties would want to give so much primary consideration to the operation of code, which is susceptible to bugs and coding errors. Thirdly, smart contract code may be required to be interpreted so as to assess its interaction with other terms of the relevant contract and also the general law. For example, smart contract code may need to be interpreted to determine whether it would be in breach of applicable laws or regulations.

There then remains the question of what principles of interpretation should apply to smart contract code. In England, the Law Commission has suggested that the test of a "reasonable coder" should apply, i.e. to ask what a person with knowledge and understanding of code would understand the coded term to mean. However, different jurisdictions may take different approaches in this regard.

Remedies

Given the automated nature of smart contracts, not all traditional remedies may be effective against them. This is particularly so where smart contracts operate on public blockchains, which are immutable. For example, remedies such as rectification, rescission or termination may simply be impossible to implement.

There may be workarounds to achieve the same practical effect, e.g. entering into an "equal and opposite" transaction as a substitute for rescission. However, that difference of there being two transactions as opposed to a rescinded transaction may have legal significance in other respects and lead to unintended consequences, which may not be ideal. For termination, there may not be any plausible workaround and the parties may be forced to wait until the contract plays itself out to its conclusion.

Conclusion

There is little doubt that the widespread adoption of smart contracts and digital asset derivatives by market participants would revolutionise the derivatives market, particularly were the technologies to be used in tandem. However, as is plain to see from the above, the good work done so far by governmental and industry bodies will need to be continued and furthered before this potentially exciting new reality comes to pass.

Jonathan Gilmour
Tel: +44 20 7295 3425 / Email: jonathan.gilmour@traverssmith.com

Jonathan Gilmour is a partner at Travers Smith and heads its Derivatives & Structured Products Group. He specialises in derivatives and structured products from both a transactional and advisory standpoint. He is widely regarded by peers and clients as one of the leading specialists in his field. He counts among his clients some of the UK's largest and most sophisticated financial institutions, investment managers, private equity houses, challenger banks and occupational pension schemes. Jonathan regularly negotiates and advises on ISDA, GMRA and GMSLA documentation as well as the impact of related regulation, including EMIR/UK EMIR and SFTR/UK SFTR. He also advises on the structure and documentation of bespoke transactions to hedge exposure to key market risks, including interest rate, inflation, FX and longevity, and advises on investment management, custody, clearing and collateral management arrangements, as well as pension scheme funding and risk transfer arrangements. Jonathan was recognised in the 2022 edition of *The Legal 500* as a "Leading Individual" in derivatives and structured products.

Tom Purkiss
Tel: +44 20 7295 3361 / Email: tom.purkiss@traverssmith.com

Tom Purkiss is an associate in the Derivatives & Structured Products Group. He advises on investment management arrangements, ISDA and GMRA documentation, fund-level hedging structures, custody agreements and collateral arrangements against the backdrop of continuing regulatory developments, including the European Market Infrastructure Regulation (EMIR) and the Securities Financing Transactions Regulation (SFTR). He acts for pension schemes, asset managers, investment funds, financial institutions, fintech companies, and corporates. Tom is also involved in the firm's *pro bono* initiatives, including the Reading and Writing Partners schemes run by Tower Hamlets council, and regularly volunteers at the Legal Advice Centre.

Travers Smith LLP

10 Snow Hill, London EC1A 2AL, United Kingdom
Tel: +44 20 7295 3000 / URL: www.traverssmith.com

Blockchain taxation in the United States

David L. Forst & Sean P. McElroy
Fenwick & West LLP

Introduction

With the invention of every new technology comes an inevitable question: how should that new technology be taxed? Generally speaking, the history of American tax law has followed a predictable pattern as it relates to the development of new technology. The new technology is invented and then the existing tax rules are adapted to provide clear answers as to how the new technology fits into the existing Internal Revenue Code (the "***Code***"). For example, as Internet became increasingly prominent in the economy, the existing tax rules were adapted as needed to the new and changing technology.[1] Transactions that utilise blockchain technology obviously were not contemplated at the time existing rules of the Code were drafted. Therefore, as with past advances in technology, adaptation of existing rules is once again needed.

Some new questions raised by blockchain technology are merely questions of interpretation. Are tokens ever currency for purposes of the foreign currency rules? Is a token a commodity for purposes of Subpart F? How do we treat transactions (like a hard fork) that are unique to blockchain technology? These are important questions, and some of those questions – and answers – will be covered by this chapter.

Some of the questions are more esoteric and require deeper exegesis of an income tax law that has existed for more than 100 years, but whose drafters could not have foreseen the substantial changes in our economy that blockchain technology is bringing. Hard forks, soft forks, airdrops, mining, staking, liquid staking, swaps – the new terminology alone highlights the complexity and diversity of transactions on the blockchain. And many of these transactions are of a kind that is different from the transactions that characterised the traditional economy before the emergence of this new technology.

Therefore, to arrive at a methodology to apply the tax law to blockchain transactions very often requires a trip to first principles – to the cases and the questions that are asked (and answered) in first-year tax law courses all across the country. For example, in applying the federal income tax to property: what is income? When does one have income? How do we think about things such as value when you are exchanging highly volatile pieces of property?

Tax authorities have offered some limited guidance (generally informal and non-precedential guidance), but the taxation of blockchain transactions remains an area with minimal formal guidance, and virtually no formal guidance from the United States. As recognised by the U.S. Internal Revenue Service (the "***Service***") in its limited and informal published guidance, generally applicable principles related to property transactions apply to cryptocurrency.

This chapter addresses some, but by no means all, of the tax issues that are currently facing cryptocurrency today. It will begin with an overview of the limited guidance from the Service on the taxation of blockchain. It will then address some thoughts on several key issues in blockchain tax today.

IRS guidance on blockchain taxation

IRS Notice 2014-21

No provision of the Code or the regulations thereunder specifically addresses the tax treatment of virtual currency. There has been some informal guidance published by the Service, most notably Notice 2014-21, published in 2014. The Notice "describes how existing general tax principles apply to transactions using virtual currency". The Notice provides this guidance in the form of answers to frequently asked questions ("***FAQs***").

In the Notice, the Service defines "virtual currency" as:

> [A] digital representation of value that functions as a medium of exchange, a unit of account, and/or a store of value. In some environments, it operates like "real" currency – i.e., the coin and paper money of the United States or of any other country that is designated as legal tender, circulates, and is customarily used and accepted as a medium of exchange in the country of issuance – but it does not have legal tender status in any jurisdiction.[2]

The Service further defines "convertible virtual currency":

> Virtual currency that has an equivalent value in real currency, or that acts as a substitute for real currency, is referred to as "convertible" virtual currency. Bitcoin is one example of a convertible virtual currency. Bitcoin can be digitally traded between users and can be purchased for, or exchanged into, U.S. dollars, Euros, and other real or virtual currencies.[3]

For purposes of this chapter, the term "cryptocurrency" shall be equivalent to the concept of a convertible virtual currency. It is unclear to the authors whether there is any token that the Service would consider "virtual currency" but not consider "convertible virtual currency".

The Notice provides the Service's position on a number of key issues in the taxation of cryptocurrency. Its first, fundamental clarification is that for federal tax purposes, virtual currency should be treated as property. Thus, general tax principles applicable to property transactions apply to transactions using virtual currency.[4] That is, basic principles of basis, gain/loss, *et cetera*, apply to virtual currency.[5] Correspondingly, in accordance with the treatment of virtual currency as property, it is not treated as currency (like a pound or a euro) that could generate foreign currency gain or loss for U.S. federal tax purposes.[6]

The Notice also states that for U.S. tax purposes, transactions using virtual currency must be reported in U.S. dollars. Therefore, taxpayers will be required to determine the fair market value of virtual currency in U.S. dollars as of the date of payment or receipt. Accordingly, a taxpayer who exchanges one type of cryptocurrency for another type of cryptocurrency (say, exchanges Bitcoin for Solana) could have to recognise gain or loss on such an exchange. Because a federal tax liability must be paid in U.S. dollars, a taxpayer with a tax liability on such a transaction would need access to U.S. dollars to pay such liability.

The Notice also touches on valuation issues, stating that if a virtual currency is listed on an exchange and the exchange rate is established by market supply and demand, the fair market value of the virtual currency is determined by converting the virtual currency into U.S. dollars (or into another real currency that in turn can be converted into U.S. dollars) at the exchange rate, in a reasonable manner that is consistently applied. There are many cases, of course, where there is no exchange on which a particular token is traded, or there is minimal liquidity of a token, which can complicate questions of valuation. And there remains the question of whether there is a distinction between the concept of a "virtual currency" and a "convertible virtual currency".

The Notice also addresses a number of other issues relevant to the taxation of cryptocurrency. The Notice addresses, without any substantive analysis, the question of whether a taxpayer

who "mines" new units of a cryptocurrency has taxable income upon the mining of the tokens, a topic to which this chapter will return.[7] The Notice also addresses information reporting requirements, and notes that payments of virtual currency are subject to general information reporting requirements.[8] Of course, myriad complications arise in how to implement information reporting requirements – this is another topic to which this chapter will return.

In response to certain countries (most notably El Salvador) adopting Bitcoin as a form of legal tender, the Service provided an update to Notice 2014-21. In that update – Notice 2023-34 – the Service clarified that:

> In certain contexts, virtual currency may serve one or more of the functions of "real" currency – i.e., the coin and paper money of the United States or of any other country that is designated as legal tender, circulates, and is customarily used and accepted as a medium of exchange in the country of issuance – but the use of virtual currency to perform "real" currency functions is limited.

Aside from this relatively minor change, the Service did not and has not otherwise altered its conclusions in the 2014 Notice.

Revenue Ruling 2019-24

Revenue Ruling 2019-24, the first revenue ruling issued by the Service on the taxation of cryptocurrency, addresses two situations. Situation (1) addresses whether a hard fork of a cryptocurrency creates taxable income under Section 61 if the taxpayer does not receive the new cryptocurrency. Situation (2) addresses whether a hard fork with an airdrop creates taxable income when the taxpayer receives the new cryptocurrency.

The Service defines several key terms in the Ruling. A "hard fork" is deemed to occur "when a cryptocurrency on a distributed ledger undergoes a protocol change resulting in a permanent diversion from the legacy or existing distributed ledger". A hard fork may result in the creation of a new cryptocurrency in addition to the old cryptocurrency. The Service defines "airdrop" as "a means of distributing units of a cryptocurrency to the distributed ledger addresses of multiple taxpayers".

The Service's analysis focuses on a key inquiry – whether the taxpayer has "dominion and control" over cryptocurrency after a hard fork. This test comes from the landmark U.S. Supreme Court case *Commissioner v. Glenshaw Glass*.[9] In that case, the Court defined "income" as "undeniable accessions to wealth, clearly realized, and over which the taxpayers have complete dominion".[10] In analysing whether the taxpayer had income upon a hard fork or an airdrop, the Court looked to this fundamental caselaw test.

In situation (1), the Service concluded that the taxpayer did not have income under Section 61 since the taxpayer did not receive new cryptocurrency and, accordingly, the taxpayer does not have an accession to wealth.

In situation (2), the Service drew a different conclusion because the taxpayer received the new cryptocurrency via an airdrop. Accordingly, the taxpayer was deemed to have an accession to wealth. Because the taxpayer is able to dispose of the cryptocurrency immediately, the Ruling holds that the taxpayer has dominion and control over the new cryptocurrency at the time of the airdrop. This dominion and control is generally established when the transaction is recorded on the distributed ledger (that is, when the transaction is recorded on the blockchain), subject to the important limitation discussed below. The Service further concluded that the taxpayer's basis in the new cryptocurrency is equal to the fair market value of the new cryptocurrency when the airdrop is recorded on the distributed ledger, and the taxpayer's income is ordinary in character.

According to the Service's interpretation, the "taxpayer does not have receipt of cryptocurrency when the airdrop is recorded on the distributed ledger if the taxpayer is not able to exercise dominion and control over the cryptocurrency". Accordingly, a taxpayer would not have dominion and control over a cryptocurrency if such cryptocurrency were in a wallet managed through an exchange that does not support the newly created cryptocurrency. The key consideration is that the Service asserts that the taxpayer has income when the taxpayer is able to transfer, sell, exchange or otherwise dispose of the cryptocurrency.

The Service further addresses some of these issues in Chief Counsel Advice ("***CCA***") 202114020. The CCA addresses the tax consequences for an individual who received Bitcoin Cash as a result of the Bitcoin hard fork on August 1, 2017. In applying the ruling of Revenue Ruling 2019-24 to the particular facts of the Bitcoin/Bitcoin Cash hard fork, the Ruling noted a few key things. First, it suggested that the Service would be flexible in taxpayers' reasonable attempts to value cryptocurrency, finding that taxpayers "can determine the Bitcoin Cash's fair market value using any reasonable method, such as adopting the publicly published price value at a cryptocurrency exchange or cryptocurrency data aggregator". This is critical because it can often be difficult, if not impossible, to determine the fair market price of crypto at the exact moment of an airdrop. It also confirmed the Service's position that dominion and control was tied to the ability to sell the token – the delivery of the token to a cryptocurrency exchange was not, in and of itself, sufficient to establish dominion and control where that cryptocurrency exchange did not support the new token.

Revenue Ruling 2023-14

On July 31, 2023, the Service issued Revenue Ruling 2023-14, which sets forth the Service's position as to when certain staking "rewards" are taxable income.

The Ruling analyses a fact pattern where a cash method taxpayer "stakes 200 units of [token] M and validates a new block of transactions on the M blockchain, receiving 2 units of M as validation rewards". The Ruling concludes that the taxpayer must include the "fair market value of the validation rewards received" in gross income during "the taxable year in which the taxpayer gains dominion and control over the validation rewards".

Our analysis of this Ruling is discussed below in our discussion of mining and staking.

Other guidance

In various other forms of informal guidance, the Service has presented its position on issues relevant to taxpayers in cryptocurrency. For example, in CCM 202035011, the Service addresses the question of crowdsourcing services. The Memorandum concludes that a taxpayer who receives virtual currency in exchange for performing a microtask on a crowdsourcing platform has received consideration in exchange for performing a service, and the convertible virtual currency is taxable as ordinary income. And in CCA 202124008, the Service states its position that exchanges of different cryptocurrencies were not like-for-like exchanges under the pre-TCJA (Tax Cuts and Jobs Act) version of Section 1031.

The Service has also issued some other forms of informal guidance. Some of this has been in the form of FAQs. These questions and answers are informal guidance that even the Service cannot rely on. Per the Service's website:

> FAQs are a valuable alternative to guidance published in the Bulletin because they allow the IRS to more quickly communicate information to the public on topics of frequent inquiry and general applicability. FAQs typically provide responses to general inquiries rather than applying the law to taxpayer-specific facts and may not reflect

> various special rules or exceptions that could apply in any particular case. FAQs that have not been published in the Bulletin will not be relied on, used, or cited as precedents by Service personnel in the disposition of cases.[11]

Key topics in blockchain tax

Although IRS guidance has only touched on a few topics in the taxation of cryptocurrency, there are numerous issues related to the taxation of cryptocurrency and blockchain transactions that are highly important and relevant to practitioners in the field. In the following section, we will discuss a few of those transactions.

Staking/mining

An area of tax law that has gained considerable attention in the past couple of years is staking. Staking is a type of transaction that only arises in the context of the blockchain. The transaction comes about due to the need for a blockchain to validate transactions recorded on that blockchain using its native token. Two approaches to this problem are mining and staking.

Mining, as used here, refers to the creation of tokens through an on-chain validation process in blockchains with a proof-of-work consensus mechanism. In proof-of-work cryptocurrencies (like Bitcoin), the process of mining requires nodes to solve computationally complicated math problems using a computer. Each node attempts to solve the problem repeatedly until one node is successful (computing a hash). With this hash, the node can then build a verified blockchain, and is able to likewise create a new token (or tokens).

Staking, on the other hand, uses a different process that results in the creation of new tokens. Staking, as used here, refers to the creation of tokens through an on-chain validation process in blockchains with a proof-of-stake consensus mechanism. The use of existing tokens and computing power together validate transactions that use other tokens native to that blockchain through a process referred as "staking". Persons use tokens native to that blockchain to engage in the staking process, which also requires computing power to validate transactions.

Through staking, individual stakers create new blocks on the public blockchain that are an immutable record of transactions on the blockchain. As new blocks are created, new tokens are created due to the actions of the staker, which in turn reflect the creation of the new blocks in the expansion of the blockchain.

As noted above, the Service provided a statement in Notice 2014-21 about mining, but has otherwise not opined on the topic.[12] But the Service (except through the government's litigation posture in the *Jarrett* case discussed below) has never addressed the question of staking.

Jarrett v. United States is a case of first impression on the taxation of native, on-chain staking on a proof-of-stake blockchain.[13] The case involves an individual – a small business owner from Nashville, Tennessee – who staked tokens on a blockchain known as Tezos.

Jarrett is arguing that new units of Tezos ("***Tezos tokens***") created through staking are created property and should therefore not be taxed until the new Tezos tokens are sold. Jarrett's argument relies on generally applicable tax principles that apply to newly created property, arguing that those principles apply to cryptocurrency tokens. As put in the Complaint:

> The federal income tax law does not permit the taxation of tokens created through a staking enterprise. Like a baker who bakes a cake using ingredients and an oven, or a writer who writes a book using Microsoft Word and a computer, Mr. Jarrett created

> property. Like the baker or the writer, Mr. Jarrett will realize taxable income when he first sells or exchanges the new property he created, but the federal income tax law does not permit the taxation of the Jarretts simply because Mr. Jarrett created new property.[14]

In December 2021, after answering the Complaint and nearing the end of fact discovery, the U.S. Department of Justice proffered a refund to the Jarretts for the full amount sought, including interest.

The District Court granted the government's motion to dismiss the Complaint on the grounds that the case is moot because the taxpayers were proffered a refund. The Jarretts have appealed this dismissal to the U.S. Court of Appeals for the Sixth Circuit. In May 2023, the Sixth Circuit heard oral argument in the case. Three business days after oral argument, the Service issued Revenue Ruling 2023-14.

As noted above, Revenue Ruling 2023-14 sets forth the Service's position with respect to staking "rewards". What the Ruling does not say is far more significant than what it does say.

First, the facts that the Service rules on do not state that the tokens are newly created property with respect to which the taxpayer is the first owner. Of course, not all staking arrangements involve newly created property. For example, there are many situations where a person engaged in staking receives tokens from a preexisting pool of tokens (and is "paid" such tokens for providing services by a governance foundation, or some other entity). To the extent the Ruling simply stands for the proposition that a taxpayer who receives preexisting tokens from another party recognises income at the time the taxpayer gains dominion and control over those tokens, we agree with the conclusion as being straightforward.

However, in a wide array of staking transactions, this simply is not how things work. The Ruling does mention, as background, that "validation rewards typically consist of one or more newly created units of the cryptocurrency native to that blockchain" – a fact pattern typical of how tokens are created by stakers on proof-of-stake blockchains – but this statement is conspicuously absent from the facts on which the Service rules in the Ruling itself.

Second, the Ruling's application of the landmark U.S. Supreme Court case *Commissioner v. Glenshaw Glass Co.* is silent as to a necessary element of the Court's holding. *Glenshaw Glass* sets forth the classic definition of income, requiring "instances of undeniable accessions to wealth, *clearly realized*, and over which the taxpayers have complete dominion".[15] The Ruling concludes that the taxpayer acceded to wealth, and states that the taxpayer has income when it gains complete dominion over the tokens, but the Ruling is conspicuously silent about clear realisation.

Thus, even if the facts posited by the Ruling are stretched beyond their most natural reading and the Ruling is construed as applying to situations where a staker creates new tokens and is the first owner of such tokens, the Ruling never concludes, as it must under *Glenshaw Glass*, that the taxpayer has a realisation event. The Ruling also fails to address a century of other caselaw and guidance that supports the non-taxability of self-created property. The Service cannot, of course, unilaterally override the Supreme Court and other judicial opinions.

Finally, we note that revenue rulings are not binding law; they merely reflect the Service's opinion of the law. Courts (and in particular the Tax Court) generally do not defer to the Service's analysis in a revenue ruling. And, to the extent the Service's analysis applies to tokens that are newly created through the staking process on a proof-of stake network, we believe the Ruling is, at best, incomplete in its analysis.

This Ruling marks the first time that the Service has stated any published position on staking. The Ruling's analysis circumvents key factual and legal issues regarding whether newly created tokens through staking should be subject to taxation at the time of creation.

DAOs

An area of increasing interest and importance within the tax law of cryptocurrency is the taxation of decentralised autonomous organisations (or "***DAOs***"). In short, DAOs are organisations constructed by rules encoded in a computer program. The program that encodes these rules is generally open source. DAOs are decentralised and are thus governed by the tokenholders.

Among other issues, DAOs raise a fundamental question of entity classification. What is a DAO, for tax purposes? Is it a corporation? A partnership? A trust? None of the above? Of course, the answer is often fact-specific, and there is a variety of arrangements that could reasonably be called DAOs. This extraordinary variance suggests that there is not (and should not be) a one-size-fits-all answer. Each DAO must be evaluated under the basic principles of tax laws.

In 2022, Senators Lummis and Gillibrand proposed legislation that would mandate that DAOs be *de facto* business entities.[16] The net effect of this would require all DAOs to be classified as either a partnership or a corporation. Again, the authors disagree with this one-size-fits-all approach. The term "DAO" does not describe a single arrangement; rather, it refers to a decentralised manner of governing the arrangement, and the underlying structure or economics of such arrangement (and the so-called "wrappers" that are used in connection with such DAOs) can vary widely.

Furthermore, DAOs with an international flavour often require an in-depth international tax analysis. One must consider whether a DAO is a corporation, a controlled foreign corporation, or a passive foreign investment company ("***PFIC***") (which we further discuss below). The application of these rules in the context of DAOs can be unclear. In the coming years, the authors expect questions about the taxation of DAOs to become increasingly prominent, and to increase in importance as this form of doing business becomes more widespread.

PFICs in cryptocurrency

U.S.-based investors in crypto enterprises often need to consider whether that investment will be considered an investment in a PFIC. The PFIC classification applies to investments in stock in foreign corporations by a U.S. person, with certain exclusions. The issue is particularly prominent within the blockchain industry because many blockchain enterprises and companies are located outside of the United States for non-tax regulatory reasons. Minority U.S. investors thus must carefully consider PFIC concerns before making an investment. In general, for an entity to be a PFIC, 50 per cent of its assets must be held for the production of passive income, or 75 per cent of its income must be passive.[17]

It is possible (particularly with market fluctuations) for an entity to have a significant proportion of passive assets even if the entity is primarily operating an active business. This has historically been a concern with cash-heavy, early-stage companies and can be a concern in the context of cryptocurrency.

Crypto loans

Another area of importance to cryptocurrency companies is how loans denominated in cryptocurrency are treated for tax purposes. Given the use of cryptocurrency as, in effect, a form of money, one type of transaction that has grown in prominence is to loan cryptocurrencies between parties in a manner similar to cash. But the tax treatment of such transactions makes loans of cryptocurrency a potential trap for the unwary.

What does it even mean to "loan" a fungible cryptocurrency token? Because cryptocurrency is generally treated as property for tax purposes, and not as money, characterisation as a

"loan" is often not appropriate. Perhaps the best analogy is to a rental of fungible units as property – say, a loan of a commodity such as ounces of gold or silver.

Another possible analogy for loans denominated in cryptocurrency might be to loans of securities. Currently, loans of cryptocurrencies do not fall under the Code Section 1058 safe harbour for loans in securities. We note that this treatment has been suggested in the proposed Lummis/Gillibrand legislation. Section 1058 provides that no gain or loss is recognised on the transfer of certain securities pursuant to an agreement that satisfies certain requirements: (i) the agreement provides for the return to the transferor of identical securities; (ii) the agreement requires that payments be made to the transferor of amounts equivalent to all interest, dividends and other distributions that the owner of the securities is entitled to receive during the term of the loan; and (iii) the agreement does not reduce the risk of loss or opportunity for gain of the transferor of the securities in the securities transferred.

Proper documentation of such "loans" is particularly important to achieve the desired tax treatment (including, for example, the proper taking into account of hard forks or airdropped property).

Information reporting

In 2021, Congress passed the first-ever bill to contain language concerning digital assets. This bill expands the current reporting requirements under Section 6045 of the Code, which requires any "brokers" to file information returns about its customers to the Service. This bill's expanded definition of "broker" would include "any person who (for consideration) is responsible for and regularly provides any service effectuating transfers of digital assets on behalf of another person". "Digital assets" are broadly defined as "any digital representation of value which is recorded on a cryptographically secured distributed ledger or any similar technology as specified by the Secretary". This bill's language is open to broad interpretation, which could obligate persons designated as "brokers" to provide the Service with information they do not actually possess.

The bill also includes several other changes to reporting requirements. First, the bill introduces the requirement that brokers report any transfer of a digital asset that is not part of a sale or exchange from an account maintained by the broker to an account maintained by a non-broker. This new requirement appears to target the transfer of digital assets from an exchange account into a cold wallet (an account not regulated by an exchange).

These requirements were scheduled to go into effect on January 1, 2023 and to apply to all transactions taking place in and after the 2023 calendar year. However, at the time of writing, the Service has not issued any guidance for the application of these rules, nor has Treasury issued proposed or final regulations.

Additionally, the bill expanded the cash reporting rules of Section 6050I to include crypto transactions of at least $10,000. The expanded reporting rules would require that any person operating a trade or business that receives payment in digital assets valued at more than $10,000 file an information return with the Service. This return would include information, such as the name, address, and social security number, of the person making such a payment. Just as in the case of the broker reporting rules, these regulations could require that individuals report information that they do not actually possess.

On August 25, 2023, Treasury and the Service released proposed regulations interpreting these rules. The proposed regulations address the treatment of gross proceeds and basis reporting by brokers in digital assets as well as the determination of amount realised and

basis for digital asset transactions. The proposed regulations expand the meaning of "effect" within the definition of broker. Existing final regulations, which interpret the law before the Infrastructure Act's amendments, provide that a person is a broker if such person stands ready to effect sales made by others and, in addition, that a person effects sales if such person is an agent for a party in a sale such that the agent *ordinarily would know* the gross proceeds from the sale.

Furthermore, the proposed regulations state that a person can effect a transaction (and thus be a broker and subject to the reporting rules) if such person "knows or is in a position to know the identity of the party that makes the sale and the nature of the transaction potentially giving rise to gross proceeds from the sale". This "in a position to know" standard represents a departure from the usual "knows or has reason to know" standard used in other parts of the Code and regulations relating to reporting. According to Treasury, "[t]he ability to modify the operation of a platform to obtain customer information is treated as being in a position to know that information".

These rules are intended to be quite expansive. Treasury and the Service expect that this clarified proposed definition will ultimately require operators of some platforms generally referred to as decentralised exchanges to collect customer information and report sales information about their customers, if those operators otherwise qualify as brokers. Treasury has explicitly stated its intent for these rules to apply to certain decentralised finance platforms.

Conclusion

Blockchain technology presents new and potentially revolutionary ways of conducting business. While many arrangements utilising blockchain technology are unfamiliar, basic principles of income tax law can often be used and adapted (and should often be used and adapted) to provide answers to the myriad questions this new technology brings. It is an exciting time for the tax law.

* * *

Endnotes

1. An example would be the application of sourcing rules to cloud computing technologies. *See* Prop. Treas. Reg. Section 1.861-19.
2. Notice 2014-21. Notably, at least two countries have granted Bitcoin legal tender status. Despite this, it seems straightforward that the Service will continue to treat Bitcoin as a "virtual currency" for purposes of Notice 2014-21.
3. Notice 2014-21.
4. *Id*. at A-1. The Service has consistently held this position in all published guidance, and the authors agree with this characterisation. *See*, *e.g.*, CCM 202035011. However, we note that in *Jarrett v. United States*, discussed later in this chapter, the government denied this in its answer. Answer, paragraph 30, *Jarrett v. United States*, No. 3:21-cv-00419 (M.D. Tenn., Aug. 27, 2021).
5. Notice 2014-21 at A-3.
6. *Id*. at A-2.
7. *Id*. at A-8, A-9.
8. *Id*. at A-12, A-13.

9. 348 U.S. 426 (1955).
10. *Glenshaw Glass*, 348 U.S. at 431.
11. https://www.irs.gov/newsroom/general-overview-of-taxpayer-reliance-on-guidance-published-in-the-internal-revenue-bulletin-and-faqs
12. *See* Notice 2014-21 at A-3.
13. The authors are counsel to Joshua Jarrett in this case.
14. Complaint, paragraph 4, *Jarrett v. United States*, No. 3:21-cv-00419 (M.D. Tenn., Aug. 27, 2021).
15. *Glenshaw Glass*, 348 U.S. at 431 (emphasis added).
16. https://www.congress.gov/bill/117th-congress/senate-bill/4356/text
17. *See generally* Section 1297 *et seq*.

David L. Forst
Tel: +1 650 335 7254 / Email: dforst@fenwick.com

David advises numerous clients in the blockchain industry on a wide array of corporate and international tax matters. David's clients in this space include protocol development teams, founders, investment platforms, cryptocurrency exchanges, and individual investors. David is counsel to Joshua Jarrett in a first-of-its-kind lawsuit addressing the tax treatment of tokens created through staking. David is a lecturer at Stanford Law School and UC Berkeley School of Law where he focuses on international taxation. David is a frequent chair and speaker at tax conferences, including the NYU Tax Institute, the Tax Executives Institute, and the International Fiscal Association. David is an editor of and a regular contributor to the *Journal of Taxation*.

Sean P. McElroy
Tel: +1 650 335 7993 / Email: smcelroy@fenwick.com

Sean advises clients in the blockchain industry on a wide array of corporate and international tax matters. He has advised numerous clients on tax issues relating to token generation events, private token sales, NFTs, decentralised autonomous organisations (DAOs), and centralised and decentralised cryptocurrency structures. Sean is a lecturer at Stanford Law School in a course on blockchain taxation, and has spoken at events hosted by the International Fiscal Association and the American Bar Association on the taxation of blockchain ecosystems.

Fenwick & West LLP

801 California Street, Mountain View, CA 94041, USA
Tel: +1 650 988 8500 / URL: www.fenwick.com

Blockchain-driven decentralisation, disaggregation, and distribution – industry perspectives

Marcus Bagnall, Nicholas Crossland, Ben Towell & Cecilia Lovell
Wiggin LLP

The disruptive power of DLT to enable the feasibility of non-centralised network structures lies in how it can address network pain points more efficiently and cost-effectively than traditional centralised means.

Introduction – blockchain's disruptive role in realising non-centralised networks

The concept of a cryptographically secured chain of blocks was first theorised in 1991.[1] The first proposal to successfully gain traction was the distributed ledger technology (**DLT**) called *blockchain*, supporting the revolutionary decentralised peer-to-peer (**P2P**) virtual currency Bitcoin.[2] DLT was initially conceived to support an alternative to traditional central bank-issued fiat. DLT is not the first application of decentralised P2P systems in response to proprietary centralised platforms,[3] and analogising DLT merely as a database undersells its true potential.[4] The disruptive power of DLT instead lies in its ability to facilitate network disaggregation, decentralisation and distribution where traditional centralised means could not.

Disaggregation is the separation of network components; *decentralisation* is the separation of control; and *distribution* is the separation of both. A crucial roadblock to non-centralised networks before DLT was the inability to make decisions, offer functionality and manage data without a central control authority – how can a network regulate distributed independent nodes, reliably maintain end-to-end functionality on a disaggregated network, or consistently enforce rules in a decentralised structure in a non-centralised manner? This is where DLT plays a crucial role in realising the potential of non-centralisation by realising viable commercial use cases.

Non-centralised networks are inherently easier to spread and harder to control, giving rise to knotty regulatory challenges. Regulators and lawmakers must navigate the intrinsic tension between retaining control and preventing harm while encouraging market competition and innovation, as well as the tension between intervening prematurely and waiting too long. Regulatory settings, civil society and other stakeholders will play a crucial role in creating the certainty necessary to support the growth and adoption of DLT-based non-centralised networks.

DLT is still in its relative infancy. We are only beginning to understand how DLT could facilitate new ways to govern networks. This chapter explores how DLT helps realise non-centralised networks by looking at how recently disrupted industries address network pain points with a non-centralised approach, together with current and potential regulatory challenges.

What is the difference between disaggregated, decentralised or distributed networks?

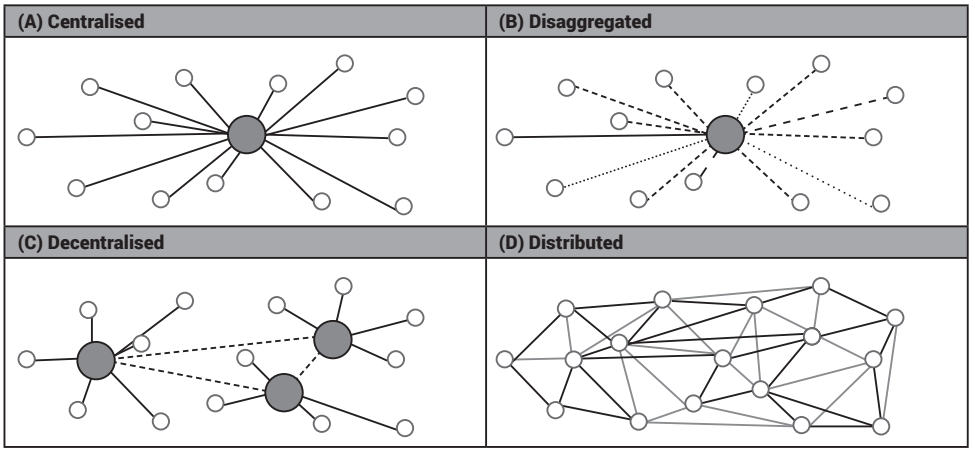
A *network* is a system of connections and interconnections to facilitate exchanges.[5] *Disaggregated*, *decentralised* and *distributed* networks describe distinct architectures with distinct legal implications. The distinguishing characteristic between these networks is the locus of control:

(A) **Centralised networks** have a central authority controlling network decision-making and information processing. P2P interactions occur as permitted by the central authority.

(B) **Disaggregated networks** are centralised networks that include interoperable functional components (whether hardware or software) that are provided, deployed, configured and managed by multiple vendors.

(C) **Decentralised networks**, also called *semi-centralised* or *semi-distributed* networks, comprise multiple independent control authorities that share network control and maintain independent decision-making and information processing. P2P interactions occur as permitted by the control authorities.

(D) **Distributed networks** have no central control authority(ies), where decision-making and information processing is shared across independent nodes in compliance with a common network protocol. P2P interactions occur as permitted by the common network protocol.



These network types can also be described along a spectrum, from centralised networks with the greatest control concentration to distributed networks with the least. Their deployment to varying degrees and in different combinations makes it commonplace to find elements of each within new network models.[6] For example:

- A geographically specific business *decentralising* its operations to scale efficiently using DLT to regulate governance rules, e.g., a company scaling up into other regions by running regional operations at a local level.
- A network operator *disaggregating* its infrastructure architecture to optimise rollout cost and flexibility using DLT for identity management, e.g., an operator rolling out a new network technology using software-defined resource allocation on commercial off-the-shelf (**COTS**) hardware.
- An infrastructure owner *distributing* its network to achieve scale by adding more independent nodes at reduced initial capital outlay using DLT to incentivise and regulate node participants, e.g., a wireless network increasing coverage by gaining more distributed independent nodes.

Evolution of distributed P2P services – ride-hailing case study

All business models need to balance the interests of value creators and extractors.[7] Organisations use centralised decision-making and policies to maximise leverage from capital assets, people and data to achieve growth and mitigate risks.[8] Centralised approaches have allowed single organisations to extract tremendous value by providing choice to value creators (service recipients) and reach to extractors (service providers).[9]

Ride-hailing platforms – disruptive but still centralised

Before the advent of ride-hailing platforms, riders wanting transport from A to B would typically either hail a government-regulated, demarcated cab or seek out a private taxi company.[10] This market has since been disrupted by ride-hailing platforms offering services centred around a mobile app to connect riders with drivers that extract a percentage of the ride value from drivers and subscription or management fees from riders. While this may *feel* P2P, it still *isn't* P2P in the same way as a decentralised crypto exchange or a file-sharing protocol – these ride-hailing platforms centrally regulate the interface between riders and drivers.

Ride-hailing platforms were disruptive by solving a problem for both *riders* (being unable to find an available taxi when needed) and *drivers* (the "dead time" between rides). Despite market dominance, household-name status, network effects, and growing revenue, the *profitability* of ride-hailing market leaders is lagging.[11]

The section above established the need to *locate* pain points in a network structure. Ride-hailing platforms extract value from value creators (i.e., from *both* riders and drivers) through: (1) imposing commissions on rides; (2) arranging rides and prioritising value extraction through pricing using a proprietary, undisclosed algorithm; and (3) excluding riders and drivers from participating in platform governance.[12] Items 1 and 2 are especially relevant to network efficiency[13] as the platform is not incentivised to allow pricing to be set entirely by ride supply and demand when its revenue depends on commission. Regulatory intervention has also proposed fare caps on rides, for example, in responding to perceived distortions from excessive surge pricing – driven also by platform value extraction – during events of acute ride demand.[14]

DLT-driven decentralised ride-hailing platforms

When mere improvements to the central node are insufficient, the whole network structure must change.[15] An alternative to centralised quasi-P2P structures involves decentralising the network: (1) drivers pay a flat subscription fee to access the platform (rather than a commission on rides set by the platform); and (2) fares for rides are set by a real-time auction model, allowing riders to choose a driver based on price, timing, and rating.[16]

DRIFE goes further by employing a decentralised autonomous organisation (**DAO**)-based model where platform operation[17] is relinquished by the "Mother DAO" to local "City DAOs" responsible for local legal compliance.[18] An internal token economy supplements the platform's subscription revenue and incentivises activity across the network.[19] DLT enables a true P2P model by using smart contracts to compute ride prices, transfer payments from riders to drivers, resolve simple disputes, handle ratings and other operations. Franchisees can determine smart contract parameters using powers granted via NFT by the Mother DAO.[20]

Challenges

The pain-point solution above could be a template for any centrally controlled P2P network facing similar challenges, such as lettings or renting, two-sided online marketplaces, car sharing, content services, or a myriad of other platform business network models in the growing gig economy.[21]

The challenges that apply to DLT-driven non-centralised P2P services are an evolution of those affecting existing centralised platform-based operators in the sharing economy. Centralised platforms consistently argue that they merely arrange for (and do not provide) the underlying substantive activity, to which regulators typically respond by imposing further centralised responsibilities on platforms. However, this regulatory approach would not be effective if applied to true distributed P2P platforms with no single control authority. Regulators would need to adopt a different approach, such as ensuring that governance tokens and dispute resolution procedures contain appropriate rules to ensure policy and market outcomes.[22]

Decentralised service provision and platform-driven P2P services have materially contributed to the rise of casual work and the gig economy. High-profile examples exist of cases seeking to arrest the erosion of employee rights accompanying the departure from centralised control structures.[23] In contrast, it appears less likely that decentralised platforms without a central control authority would be held as an employer.

How blockchain is disrupting content and platforms

Platform-based content distribution services have disrupted the creative economy through the evolution of the internet and the resulting adaptation of global frameworks. These platforms typically offer content creators hosting, security, payment processing, distribution and monetisation options, and a level of legal protection. Instant reach to global audiences allows creators to focus on content. In return, platforms exercise a degree of control over the reach and monetisation of creator works, which makes creators dependent on platforms and the specific rights or features they make available (or take away).[24]

A recurring theme describing the disruptive power of DLT is the application of blockchain technology in the music industry, realising tokenisation of music rights and royalty distribution based on actual use of music. In contrast to the traditional complex of publishers, record labels, agents and channels intermediating artists and audiences, blockchain technology enables the monetisation of artist-fan engagement with trustless on-chain transparency.[25]

Content monetisation

Platform content distributors typically generate revenue centrally through paid subscriptions and monetising user data through advertisements. While advertising will remain a crucial monetisation method for non-centralised content platforms, a DLT structure can distribute benefits between content creators, consumers and other stakeholders without a value-extracting centralised platform.

There are several examples of this occurring regarding music content. *OPUS*[26] allows listeners to stream music tracks and distributes royalties to artists using their native OPT token by collecting statistics of the played songs, allocating a substantial percentage of revenue to artists and offering the opportunity for fans to generate an income as well by becoming part of the artist's social circle in the platform. *Lissen* has similar features and adopts an on-chain, user-centric approach to calculating and distributing royalties allowing listeners to directly and transparently support their favourite artists.[27] *Audius* also allows artists to earn AUDIO tokens as a supplemental royalty stream.[28] *Itoka*, a decentralised music platform to tokenise AI-generated music content, allows creators to independently license that content and receive compensation every time the track is played.[29]

Challenges

While DLT-driven platform decentralisation can be used to solve network pain points, managing digital rights and creator monetisation in a practical, commercially viable manner is as much a legal challenge as it is a technical and industry one. Centralised platforms will

remain relevant for the foreseeable future, with many DLT-based proposals still heavily reliant on traditional platforms to achieve reach.[30]

Protecting the interests of rightsholders has become a particularly pressing concern as content becomes more accessible through platforms. While criticisms persist regarding how truly decentralised platforms could ever effectively enforce the interests of rightsholders, decentralised solutions to monitor, report and assist with enforcement are being rapidly developed to be deployed with DLT-based content distribution models.[31]

How non-centralised platforms manage the interests of rightsholders also depends on the nature of the DLT itself, with the scope of rights afforded to tokenholders being a key determinant for its regulatory treatment. A DLT-based music platform may find itself needing to comply with financial services or crypto-specific regulation if its native token is a regulated cryptoasset and it provides any accompanying fiat-crypto exchange or custodial wallet services.[32]

Given existing regulatory frameworks, DLT-driven non-centralised music platforms raise several legal and regulatory challenges:

- **Regulatory compliance and enforcement**. Existing platform regulatory frameworks assume a centralised network, where the relevant platform control authority retains control and rights over content and activities occurring on the platform. This is also the basis for the control authority observing certain obligations and being liable to provide remedies. Recent regulatory responses seek to protect end-users through *more* centralised control over content.[33] Non-centralised networks instead facilitate networked content distribution with less (or no) control over what a content consumer sees, which demands a radically different approach to regulation to achieve desired policy outcomes. This could be achieved, for example, by imposing rules on protocols regulating on-chain activities of DLT-based platforms or requiring that certain minimum functionality remains centralised with a control authority responsible to the regulator.
- **Challenges with using DLT as a record of digital asset legal rights**. It will be impossible (or at least undesirable) to use an open, permissionless DLT record to establish definitive legal title or rights for all digital assets, such as creating and enforcing intellectual property rights. This reality may be a hard edge to adopting DLT-based digital assets on non-centralised content platforms until further statutory rules recognise legal title to digital assets.[34] Many incompatibilities arise from DLT-based legal rights across different legal areas that would need to be addressed on a case-by-case basis. For example, from a data protection perspective, DLT is unlikely to be compatible with (a) GDPR "controller" and "processor" roles, and (b) rights to erasure, rectification, portability, and consent withdrawal.[35] There are also challenges to removing or rectifying DLT-based content once it is shared (particularly content that includes personal data) in a DLT-driven platform.[36]
- **Due diligence will be critical**. It will be even more important when dealing with non-centralised platforms to pay close attention to the terms and conditions governing engaging with and creating content on DLT-driven platforms. The nascency of DLT means there is little precedent for their effectiveness nor a critical mass to describe what is accepted market practice. Emerging DLT-driven platform operators may also find themselves inadvertently captured by regulations not intended for this purpose.[37] In the likely absence of widespread industry cooperation, regulations will be required if the goal is to achieve minimum standards on platform terms, mandatory industry codes of practice, and protocols to ensure consistency, reliability and interoperability between platforms.[38] In the meantime, due diligence of the DLT platform and any digital assets purported to be created or supported by the platform will be critical for potential participants.

Non-centralised telecoms networks and infrastructure

Telecommunications network operators are facing unprecedented pressures to free up their balance sheet to fund costly network upgrades, deploy new technologies and find design efficiencies to compete for market share.[39] Operators and infrastructure providers are traditionally heavily centralised and subject to onerous industry and service-specific regulations. Operators in many markets have suffered from a lack of investment, resulting in impaired network performance and leaving many citizens underserved, particularly those in rural and remote areas.[40] The barrier to entry for new players is high, while regulators closely scrutinise proposed consolidations being acutely aware of anti-competitive effects.[41] OpenRAN has emerged as the industry's application of network disaggregation principles to reduce cost and increase efficiency, capacity and interoperability for mobile networks, particularly in the roll out of 5G mobile networks.[42] DLT solutions now feature in operator efforts to improve network costs, resilience, efficiency and sustainability in a non-centralised approach to address the *last mile issue*.[43]

OpenRAN

Under traditional network architecture, a radio access network (**RAN**) uses proprietary hardware (a remote radio unit or **RRU**) attached to a mobile tower to exchange signals with user equipment. The RRU connects with baseband units, again comprising proprietary hardware and software, which send data between the base station and the operator's central unit or core network. These technologies are proprietary to vendors and, historically, limited efforts have been made to ensure they are interoperable or can be componentised by operators.

OpenRAN applies disaggregation to this process by enabling operators to run baseband functions as *software* and by facilitating non-proprietary RAN solutions on *vendor-neutral platforms*. This has several benefits, including:

- encouraging competition, innovation and more diversified supply chain development;
- cost efficiency through enabling operators to use COTS hardware and components;
- flexibility and scalability via OpenRAN's modular and software-driven architecture, allowing for operators to scale their networks and adapt to demands; and
- faster deployment of new features and reduced time-to-market.

The rollout of OpenRAN has not been without its challenges, which, alongside fears relating to the maturity of the solution preventing players from taking their initial steps, are reminiscent of concerns raised regarding non-centralised network solutions more generally:

- **Enabling interoperability**: COTS suppliers will need to meet common standards to ensure seamless integration, requiring vendor collaboration and testing to ensure compatibility.[44]
- **Ensuring privacy, security and resilience**: network disaggregation involving multiple vendors introduces security vulnerabilities and issues stemming from vendors applying different standards. This underscores the need for robust and consistent security protocols and audit procedures to identify and address potential threats.
- **Ecosystem immaturity**: while OpenRAN is at a nascent growth phase, it will take time for operators to find vendors with sufficient sophistication, or they may become dependent early on a specific vendor or integrator for support as the market matures.
- **Standardisation**: the process of achieving consensus on standardised protocols and interfaces takes time and, without clear and collaborative leadership from government and all ecosystem participants, disagreements on common standards could lead to delayed fractured development.

The key to enabling OpenRAN software and hardware disaggregation is open, common interface protocols and hardware specifications to avoid operators from being locked to a specific vendor. A number of these discussions are already taking place, including the O-RAN Alliance[45] recently agreeing on fronthaul specifications to encourage OpenRAN rollout.[46]

Realising the full potential of disaggregated networks requires close cooperation between industry and government to ensure appropriate policy settings, incentives and safeguards. For example, the UK government has awarded £80 million for OpenRAN projects, with a focus on hardware and software that enables "enhanced development and adoption of open and interoperable technology".[47]

Telecoms security regulation is also another critical factor in the push towards OpenRAN. The UK government and other governments in key markets have directed telecoms operators to remove equipment in their critical networks supplied by designated high-risk vendors on security grounds. As a result, operators have been incrementally replacing legacy single-vendor network equipment with disaggregated vendor OpenRAN systems.[48] Initial testing by Vodafone across 16 sites in the UK indicated that OpenRAN outperformed legacy RAN technology "in call success rates, as well as in download and upload speeds across multiple spectrum frequencies".[49] The embedded interoperability of OpenRAN systems allows operators to explore further network enhancements previously not possible with single-vendor legacy RAN systems.

Use of blockchain to secure processes in the telecoms sector

The Internet of Things raises significant security and data concerns that can leave both users and suppliers exposed to fraud vulnerability. DLT offers a solution to these issues through built-in features protecting the integrity and immutability of data stored on the distributed ledger. For example, Vodafone's *Digital Asset Broker* platform[50] is a decentralised framework platform enabling the "Economy of Things", providing users with a secure platform to interact and transact with each other directly and automatically. The Digital Asset Broker is supported by a blockchain SIM card, which facilitates identification by assigning a unique SIM to each device and storing user data on a decentralised encrypted blockchain network. DLT is also being considered for other trustless systems requiring transparency, certification and automatic settlement, e.g., for Mobile Number Portability, allowing customers to switch telecoms operators while retaining their existing number, and for international roaming and inter-carrier transactions.[51]

Challenges

Disaggregated network architecture is revolutionary for operating mobile networks, fundamentally changing resource deployment, using technology to achieve efficiencies and vendor collaboration to achieve component interoperability. Distributed networks are a step even further toward liquid network functionality, but with greater coordination, management and supervision challenges to overcome. The underlying question remains as to who will be ultimately responsible for compliance and regulatory obligations in an ecosystem with multiple players:

- **Regulatory compliance and enforcement**: in the UK, electronic communications networks and service providers must comply with the General Conditions[52] (**GCs**) laid out by Ofcom. Compliance with the GCs by non-centralised networks would be cumbersome and administratively burdensome,[53] and certain GCs would be impossible to ensure compliance without the network retaining certain centralised functions.[54] Equally, distributed networks deliberately lack a central control authority typically

responsible for ensuring proper network function and observing consumer protection obligations. Regulations for non-centralised communications networks would need to adopt a different approach to ensuring end-user outcomes to reflect the absence of a central control authority; for example, regulations requiring that common protocols ensure minimum network performance and reliability standards and appropriate dispute resolution mechanisms.

- **Security and lawful intercept**: as noted above, non-centralised communications networks involving multiple hardware vendors, network participants and distributed control raise significant network security and resilience concerns. Many jurisdictions are implementing enhanced security rules to protect networks, devices and users against adverse actors.[55] Participants responsible for non-centralised network nodes would also face challenges complying with lawful intercept requirements, given that encryption and traffic aggregation render network participants unable to identify individual data packets.[56] Non-centralised networks would likely need to maintain specific centralised processes to ensure compliance with security requirements.
- **Backhaul and network costs**: non-centralised networks rely on ubiquitous broadband connectivity for network nodes to obtain backhaul. Existing non-centralised network participants often use their residential broadband service (mobile or fixed) for backhaul. Not all retail internet service providers (**ISPs**) prohibit their customers from using residential broadband services for this purpose.[57] As non-centralised networks proliferate and the amount of traffic to support them increases, ISPs may well prohibit customers from using residential broadband services for third-party network backhaul and respond with measures justified by increased network utilisation and to protect revenues, such as requiring customers to take up more expensive "business" plans with higher capacity and service commitments.[58] Depending on prevailing public policy priorities, regulatory intervention may be necessary depending on the geography of non-centralised nodes to ensure continuity[59] and that those participants responsible for network propagation and utilisation bear their share of responsibilities and costs.[60]

Regulatory policy response to DLT-driven disruption

DLT-driven non-centralised networks give rise to many policy and regulatory challenges. The lack of a central control authority means that regulators may struggle to identify who they must target with an authorisation regime. In some jurisdictions, decentralised exchanges have led to regulators targeting those already within their purview (e.g., traditional banks or payment processors) in effect to restrict the flow of transactions into the decentralised economy.[61]

Ideally, these challenges will be met with timely, principled, digitally native and cross-disciplinary regulatory approaches that collaborate with all sector stakeholders to ensure that policy settings "get it right" early on. The breadth of DLT solutions and potential non-centralised network functionality deployed across various sectors of the economy will also require cooperation between regulators from multiple policy areas in multiple jurisdictions to ensure a consistent approach.[62] New laws and regulations explicitly addressing DLT-driven non-centralised networks will ultimately be needed to comprehensively regulate new network structures supported by DLT-based digital assets.[63]

The UK government has articulated its ambition to position the UK as a leading global hub for DLTs and crypto investment.[64] Recognising DLT activities and implementing targeted laws, regulations and policy guidance is crucial to enhance market trust, provide legal certainty, improve market operation by encouraging innovation, and prevent harm.[65] It will

also help create certainty, drive adoption and unlock the application of DLT in realising non-centralised networks. There has also been a focus more recently in the UK on the way that cryptoassets are *marketed*,[66] with the aim of allowing innovation while protecting consumers and retail investors against specific harms.

The recent regulatory response to tech disruptors and DLT applications to date gives valuable insight into the potential legal and regulatory challenges posed by the widespread adoption of DLT-driven non-centralised network structures:

(1) **Evolution of English law in response to DLT**. English common law is sufficiently flexible, dynamic and resilient to continue evolving to accommodate digital assets. English courts have already handed down many judgments in DLT-related disputes, illustrating how the common law system can readily adapt to the realities of non-centralised networks to meet litigants' needs. Most disputes so far have involved the claimant allegedly losing access to, or being defrauded of, their cryptoassets by adverse actors due to hacking or a DLT code exploit. Cryptoassets (including cryptocurrency and NFTs) are considered *property* under English law,[67] which may be bought and sold as well as held on trust,[68] and gives rise to remedies for property owners, such as the right to obtain injunctions.[69] While this recognition so far assists parties seeking to recover their lost cryptoassets, it remains an extension of existing common law principles to scenarios involving DLT-based digital assets. That being said, English common law does not yet recognise a general fiduciary or tortious duty of care owed by software developers to cryptoasset owners requiring developers to prevent hackers from causing harm or even to implement software patches to address an exploit in the DLT code to enable a cryptoasset owner to retain lost cryptoassets.[70] Longer term, statutory recognition of a separate class of DLT-based digital assets with specific regulations regulating its use, protection and commercialisation will help create certainty and profoundly impact the adoption of DLT-based network non-centralisation.[71] The UK's policy position and clear measures to support network disaggregation also serve as a useful blueprint for broader policy positions to support DLT-based non-centralised networks more generally.

(2) **Functional equivalence**. DLT-based network non-centralisation demands a different approach to regulation to achieve the same policy outcomes as regulation applicable to centralised networks. For example, the rise of the platform-driven digital economy eventually led to regulations ensuring equivalent treatment of in-person and online activities.[72] DLT-driven non-centralised networks should be regulated to result in functionally equivalent regulatory treatment to centralised networks. This may require a radically different approach; extending existing principles currently applicable to mature industries may risk overregulating a nascent industry and stifling DLT-driven innovation. For example, recognising DAOs as a new category of legal entity with personhood, while at the same time achieving functional and regulatory equivalence with existing categories of corporate entities.[73] As DLT is applied in further industries, more complications are arising regarding reconciling on-chain and off-chain activities that will require both technical and regulatory solutions and updating what is considered a regulated cryptoasset, as regulations focused on money laundering or financial services are unlikely to remain fit for purpose.[74]

(3) **Jurisdictional consistency**. Products and services offered via the internet challenged traditional rules regarding relevant jurisdiction and territorial application. This will become even more challenging when DLT-based distributed networks are everywhere all at once with no central location. English courts have held that territorial jurisdiction

is determined by the place where the cryptoasset owner is domiciled.[75] But, aside from the recognised right for a UK-domiciled litigant to obtain freezing orders against crypto exchanges to preserve their stolen cryptocurrency, regulatory bodies and lawmakers in jurisdictions globally must ultimately work together on achieving consistent rules to avoid forum shopping and regulatory arbitrage arising in respect of activities conducted on non-centralised networks, while also remaining sensitive to local norms and requirements.

Conclusion

Through network disaggregation, decentralisation and distribution, network operators can offer services and coverage more efficiently, faster and at a reduced cost. DLT plays a crucial role in realising non-centralised networks to provide an alternative to centrally controlled networks, fostering competition and reducing cost, and ultimately distributing benefits across more ecosystem stakeholders.

Regulation has a role to play as an enabler of digital transformation. How DLT-driven non-centralisation will impact different industries and the extent and speed of disruption varies significantly between sectors, due in no small part to the regulatory response to issues arising in each jurisdiction.

As with any nascent and disruptive technology, most players are slow to adopt it, and overregulation can threaten innovation. Complexity is often a key blocker with DLT adoption; the relative advantage must outweigh the solution's complexity.[76] Perceived relative advantage and output observability play an essential role in adoption and regulation, presenting a cyclical issue as businesses and regulators refuse to take the plunge until they see others benefit.

The regulatory frameworks have so far generally responded to technology disruptors by imposing *more* centralised obligations to ensure policy outcomes. Many of these frameworks do not react well to non-centralised networks absent a central controlling authority or location. Regulators and lawmakers will need to develop new frameworks, both cross-functionally and cross-border, to address DLT-driven non-centralised network structures to ensure against market failure and achieve policy outcomes.

* * *

Endnotes

1. Theorised by Stuart Haber & W. Scott Stornetta, in their publication "How to time-stamp a digital document" (https://link.springer.com/content/pdf/10.1007%2F3-540-38424-3_32.pdf).
2. "Bitcoin: A Peer-to-Peer Electronic Cash System" (https://bitcoin.org/en/bitcoin-paper), "Satoshi Nakamoto", 31 October 2008.
3. BitTorrent, a popular P2P file-sharing protocol, was invented in April 2001.
4. DLT is an inefficient, slow, and expensive way of storing data compared to traditional databases. Newer approaches to consensus mechanisms are changing this as we move further away from proof-of-work (mining)-based networks. Ethereum, for example, has recently transitioned to a proof-of-stake mechanism: *The Merge* (https://ethereum.org/en/upgrades/merge).
5. *Network* as defined by Cambridge Dictionary (https://dictionary.cambridge.org/dictionary/english/network). *Network* may be more usefully defined by its application – a physical network moving people across transport links, a communications network

exchanging information between computers, or a relationship network amongst a group of people. This chapter considers *networks* in the broadest sense of the word.

6. Examples beyond those discussed in this chapter include many cryptocurrencies, such as Bitcoin and Ethereum, which are both distributed and (largely) decentralised; *Chain* (https://chain.com) – a permissioned (i.e., not publicly accessible) cloud blockchain infrastructure solution uses a decentralised and distributed infrastructure protocol to enable organisations to build financial services; and *Patientory* (https://patientory.com) – a health data management service that integrates a blockchain-enabled platform via a decentralised app for the employment of its distributed application software.
7. The more "networked" a business, the harder the practice of extracting value without reciprocation, and the more propensity for inefficiency and rent-seeking behaviour.
8. See further: "To centralize or not to centralize?" (https://www.mckinsey.com/business-functions/people-and-organizational-performance/our-insights/to-centralize-or-not-to-centralize), McKinsey & Company, 1 June 2011; "Emergent centralization due to economies of scale" (https://medium.com/@clemahieu/emergent-centralization-due-to-economies-of-scale-83cc85a7cbef), Colin LeMahieu, 30 October 2018.
9. In the case of double-sided marketplaces facilitated by platforms, from the perspective of the platform the value creators are *both* the provider of the actual service and the recipient of the service.
10. Private taxi companies faced limitations in most jurisdictions, including the inability to offer hailing or having to meet specific registration requirements. See, for example, the UK's *Statutory Taxi and Private Hire Vehicle Standards (2020)* and the *Private Hire Vehicles (London) (Operators' Licence) Regulations 2000*, targeted largely at platform-based private hire vehicle operators.
11. Distortions to demand were exacerbated also due to responses to the COVID-19 pandemic. Some speculate that their business model is built upon an overconfident bet on driverless technology – see, for example, Aaron Benanav, "Automation and the Future of Work" (2020).
12. DRIFE White Paper (https://drife.gitbook.io/white-paper). Arguably, incentivising loyalty via tokenomics rather than pure pricing and service quality is counter to the aim of an efficient market, but ultimately there is still a platform with a customer base to build.
13. Transparency, open governance, and incentivised loyalty are better described as potential by-products of network redesign.
14. Fare caps are often discussed by reference to a terrorist attack in Sydney in 2014 in which prices surged as riders sought to leave the city, prompting an argument for capping ride fares to an "ethical" level.
15. DRIFE White Paper (https://drife.gitbook.io/white-paper).
16. As opposed to being determined centrally by the platform.
17. Including security, development, customer feedback, and referrals.
18. A council of 200 "elite" members make decisions on key global strategic vision – such members being holders of the DRIFE Council NFT – while local decisions are taken by the City DAOs and holders of the DRIFE Franchise NFT. The platform's subscription revenue is then supplemented by its token allocation. This has the additional purported benefit of allowing local governance networks to capitalise on local market understanding.
19. The foundation proposes to retain 20% of tokens. Tokens are then used throughout the tech ecosystem, with their value potentially being driven by the service's uptake.

20. DRIFE proposes to offer geo-bounded regions franchised as NFTs and governed from a local compliance perspective by City DAOs. Franchise NFTs are acquired in a similar way to choosing a validator in a proof-of-stake network, i.e., the more DRIFE tokens a bidder stakes, the more likely they are to acquire the franchise NFT and take over local operations.
21. See the UK Department for Business, Energy & Industrial Strategy report on "The characteristics of those in the gig economy" (https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/687553/The_characteristics_of_those_in_the_gig_economy.pdf).
22. See, for example, Rule 4 of the DAO Model Law requiring that, for a DAO to benefit from corporate personhood and mitigate risks to tokenholders, the DLT code underlying the DAO must be open source, publicly available, subject to audit and meet minimum quality standards.
23. See, for example, *Uber BV and ors (Appellants) v Aslam and ors (Respondents)* [2021] UKSC 5, holding that drivers are to be recognised as workers with minimum wage and paid holiday entitlements.
24. Make the most of the creator economy (https://www.forbes.com/sites/theyec/2022/07/18/make-the-most-of-the-creator-economy/?sh=3c636ca16e99).
25. See, for example, Lissen (https://www.lissen.live) adopting a user-centric model to calculate and distribute royalties based on the actual amount of time a user spends listening to a particular artist's music rather than total usage across a platform, with calculation data recorded on-chain to ensure transparency.
26. OPUS White Paper (https://opus.audio/whitepaper.pdf).
27. See Lissen – Royalties (https://www.lissen.live/help/royalties).
28. Audius – A Decentralised Protocol for Audio Content, White Paper (https://whitepaper.audius.co/AudiusWhitepaper.pdf).
29. See, for example, AI music content generated by Meta's MusicGen (https://huggingface.co/spaces/facebook/MusicGen).
30. For example, in August 2021, Audius partnered with TikTok allowing users to share Audius songs in their TikTok videos, allowing artists to amplify their reach. Google has updated its Play Store policy to allow more blockchain-based apps and integrate digital assets like NFTs into their games, which, until recently, have been largely prohibited (https://support.google.com/googleplay/android-developer/answer/13607354).
31. See, for example, the C2PA alliance implementing technical standards to certify media content provenance (https://c2pa.org).
32. The principal crypto-specific law in the UK is the *Money Laundering, Terrorist Financing and Transfer of Funds (Information on the Payer) Regulations 2017* (**MLRs**). The MLRs regulate businesses providing in-scope services in respect of cryptoassets, such as cryptoasset exchanges and custodial wallets. Cryptoassets are defined as "a cryptographically secured digital representation of value or contractual rights that uses a form of distributed ledger technology and can be transferred, stored or traded electronically". This is often interpreted to pure collectible tokens, as the scope of "rights" that are offered to tokenholders expands, understanding what is meant by a representation of contractual rights in relation to a token is paramount.
33. Ofcom has been designated in the UK as the regulator for harmful online content. In the EU, the adoption of the Digital Services Act imposes active obligations on online platforms to protect users and mitigate risks (including those stemming from the structure of the content distribution itself). The law also requires large platforms to provide remedies to users for certain harms.

34. A new third category of property of "digital assets" has been recognised under English law – see further Law Commission report on Digital Assets (https://www.lawcom.gov.uk/project/digital-assets/#related).
35. See a wider discussion here: https://www.wiggin.co.uk/insight/blockchain-and-the-gdpr
36. Compliance with such requirements will heavily depend on the relevant underlying DLT protocols; for example, if content is token-driven, then the protocol may need to include a mechanism to "burn" tokens to comply with erasure requirements.
37. For example, an NFT or other cryptoasset granting the tokenholder rights akin to a security will likely become subject to financial services regulations and capture DLT platforms regarding any activity relating to the offer or exchange of such cryptoassets.
38. Regulatory authorities are already looking at standardisation and interoperability from a platform perspective in existing markets. See, for example: European Parliamentary Research Service report, "Metaverse opportunities, risks and policy implications" (https://www.europarl.europa.eu/RegData/etudes/BRIE/2022/733557/EPRS_BRI(2022)733557_EN.pdf), considering standardisation and interoperability for metaverse technical standards and protocols; and CMA – Online platforms and digital advertising market study (https://www.gov.uk/cma-cases/online-platforms-and-digital-advertising-market-study#full-publication-update-history) to establish a pro-competition framework to address issues identified in the operations of online platforms.
39. How telcos can succeed in launching new businesses beyond connectivity (https://www.mckinsey.com/industries/technology-media-and-telecommunications/our-insights/the-next-telco-battleground-network-experience-and-competitiveness); The next telco battleground: Network experience and competitiveness (https://www.mckinsey.com/industries/technology-media-and-telecommunications/our-insights/the-next-telco-battleground-network-experience-and-competitiveness).
40. This has led to initiatives specifically targeting the roll out of telecoms infrastructure in rural areas; for example, the Shared Rural Network in the UK is a collaborative project that aims to increase coverage in rural areas that have not seen investment due to small customer bases hindering competition.
41. Historically, Ofcom has opposed proposed consolidations, blocking the most recent attempt in 2016 for a merger between O2 and Three. However, in a recently published discussion paper, Ofcom updated its future approach to mobile markets, stating that it is "clarifying" its position on market consolidation, possibly due to concerns around growing demand from end-users: Ofcom's future approach to mobile markets (https://www.ofcom.org.uk/__data/assets/pdf_file/0027/231876/mobile-strategy-discussion.pdf).
42. *OpenRAN critical to addressing supply chain resilience and realising 5G's full potential* (https://www.wiggin.co.uk/insight/open-ran-critical-to-addressing-supply-chain-resilience-and-realising-5gs-full-potential), Wiggin LLP, 23 August 2022.
43. The last mile issue concerns the prohibitively expensive nature of adding new infrastructure to the last segment connecting end-users to an access network. 5G rollout has also been adversely affected in many jurisdictions, particularly in urban areas, due to a combination of high tower lease and upgrade costs and limited available capacity at tower sites already occupied by 3G/4G equipment.
44. Such testing is taking place in a number of interoperability labs, one ran by O-RAN Alliance and another funded by Ofcom and DCMS. Sonic Labs: https://www.digicatapult.org.uk/expertise/programmes/programme/sonic
45. O-RAN Alliance members: https://www.o-ran.org/membership

46. This specification was to help fix a key barrier to the adoption of OpenRAN in high-performance 5G networks, that being unsatisfactory support for massive MIMO antenna arrays, which are key to increasing 5G capacity and coverage.
47. Open Networks Ecosystem Competition (https://www.gov.uk/guidance/open-networks-ecosystem-competition#full-publication-update-history).
48. For example, Vodafone announced that it would replace Huawei equipment with OpenRAN solutions at approximately 2,500 sites across Wales and the southwest of England by 2027 (https://www.vodafone.co.uk/newscentre/press-release/volume-deployment-of-openran-for-2500-sites-begins).
49. Vodafone, *Huge network upgrade begins as Vodafone finishes OpenRAN tests* (https://www.vodafone.co.uk/newscentre/news/huge-network-upgrade-begins-as-vfuk-finishes-openran-tests).
50. Digital Asset Broker by Vodafone (https://www.vdigitalassetbroker.com/#solutions).
51. GSMA holds GSMA eBusiness Network Accelerator trials for automated wholesale roaming settlement and improved cashflow (https://www.gsma.com/newsroom/press-release/omantel-and-telkomsel-sign-up-to-gsma-blockchain-trials-for-optimised-roaming-operations/#:~:text=Blockchain%20pioneers%20and%20roaming%20partners,go%20live%20in%20June%202023).
52. General Conditions of Entitlement (https://www.ofcom.org.uk/phones-telecoms-and-internet/information-for-industry/telecoms-competition-regulation/general-conditions-of-entitlement).
53. For example, non-centralised networks will particularly find it difficult to ensure connectivity to emergency services. *General Condition A3* regards ensuring the fullest possible availability of public communications services at all times, including in the event of a disaster or catastrophic network failure, as well as uninterrupted access to emergency organisations. Where a network is dependent on individually owned hotspots to provide coverage, there is a risk of loss of coverage due to a power outage, or where users enter "not-spots", i.e., areas where there is no coverage.
54. For example, non-centralised networks would have no ability to agree arrangements with emergency services organisations to ensure that services can be restored. *General Condition A4* requires all communications providers who provide voice communications services, or a public electronic communications network over which these services are provided, to agree arrangements with emergency organisations and other public authorities to ensure the provision or rapid restoration of networks and services in the event of a disaster. It would not be feasible for a non-centralised network to require each node owner to either maintain and activate back-up power or enter into an agreement with emergency organisations to preferentially restore power to hotspot locations.
55. For example, see the UK's *Product Security and Telecommunications Infrastructure Act 2022* (https://www.legislation.gov.uk/ukpga/2022/46/contents/enacted).
56. For example, Helium is a decentralised wireless network providing mobile connectivity that runs end-to-end (between the device and corresponding internet-hosted router) encryption that scrambles messages, meaning not even hosts can read messages. Data sent from devices is fingerprinted, and it is that fingerprint that is stored on the blockchain. See further: Helium White Paper (https://www.securities.io/helium-whitepaper). Pollen, another decentralised mobile network, provides SIMs that encrypt all user data traffic between user equipment, the radio network, and the mobile core. Where the mobile core delivers traffic to the internet

(the *internet egress point*), user traffic can be monitored from that point onwards and intercepted by parties conducting network surveillance and traffic analysis, including ISPs and governments. See further: Pollen White Paper (https://assets.website-files.com/61bcdf68fb5dc56d13dd117e/61f94f5e3659b7381a6a1750_Pollen%20Whitepaper%200.0.1.pdf).

57. For example, Plusnet requires that users only use their services for "personal use in the UK", explicitly stating that users should not use the services to run their own business, but that "occasional home working is okay": Plusnet Terms and Conditions (https://www.plus.net/help/legal/terms).
58. For example, Virgin Media requires that internet access is for private use by members of a household only and must not be used for "activities not reasonably expected of someone using the internet for domestic purposes". Virgin Media states a user *should* purchase the Virgin Media Business service if their use goes beyond that stated: Virgin Media Terms and Conditions (https://www.virginmedia.com/legal/fibre-optic-services-terms-conditions).
59. For example, if there is a concentration of distributed nodes in a particular geographic area served by one ISP.
60. The EU's Commissioner Vestager stated that "there is an issue that we need to consider with a lot of focus, and that is the issue of fair contribution to telecommunication networks … Because we see that there are players who generate a lot of traffic that then enables their business but who have not been contributing actually to enable that traffic. They have not been contributing to enabling the investments in the rollout of connectivity": Reuters (https://www.reuters.com/business/media-telecom/eus-vestager-assessing-if-tech-giants-should-share-telecoms-network-costs-2022-05-02).
61. See, for example, Argentina's ban on payment providers offering crypto transactions or facilitating crypto services.
62. See, for example, the cooperation statement between the CMA and Ofcom on harmonising their approach to online safety and competition in digital markets, with both departments agreeing to take complimentary approaches and balance their objectives: Online safety and competition in digital markets: a joint statement between the CMA and Ofcom (https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/1090501/Online_Safety_and_Competition_in_Digital_Markets_-_Joint_Statement_14.7.22.pdf).
63. The Law Commission's July 2022 consultation paper on Digital Assets, section 11 referring to Consultation Question 18 (https://s3-eu-west-2.amazonaws.com/lawcom-prod-storage-11jsxou24uy7q/uploads/2022/07/Digital-Assets-Consultation-Paper-Law-Commission-1.pdf).
64. The UK government announced its plans in April 2022 to position the UK as a global hub for cryptoasset technology and investment: Press release (https://www.gov.uk/government/news/government-sets-out-plan-to-make-uk-a-global-cryptoasset-technology-hub).
65. See, for example, the FCA's mission statement (https://www.fca.org.uk/publication/corporate/our-strategy-2022-25.pdf).
66. See, for example, the FCA's new marketing rules (https://www.fca.org.uk/news/press-releases/fca-introduces-tough-new-rules-marketing-cryptoassets).
67. *AA v Persons Unknown* [2019] EWHC 3556 (Comm), which has been cited by over a dozen cases since including the Court of Appeal to support the conclusion that a particular digital asset is capable of being personal property.

68. *Ion Science Ltd v Persons Unknown and ors* (unreported, 21 December 2020); *Zi Wang v Graham Darby* [2021] EWHC 3054 (Comm).
69. *Vorotyntseva v Money-4 Limited* [2018] EWHC 2596; *AA v Persons Unknown, Re Bitcoin* [2019] EWHC 3556; *Fetch.ai Ltd and anr v Persons Unknown Category A and ors* [2021] EWHC 2254 (Comm); *Lavinia Deborah Osbourne v Persons Unknown and Ozone Networks* [2022] EWHC 1021 (Comm).
70. *Tulip Trading Limited v Bitcoin Association for BSV* [2022] EWHC 2 (Ch).
71. See, for example, recommendations in the Law Commission's June 2023 report on Digital Assets recommending the creation of a panel of crypto token experts to provide non-binding guidance on the further development of the common law, as well as recommendations for specific legislative intervention to address certain remaining "highly nuanced and complex" areas of uncertainty.
72. See, for example, the increase in scrutiny of online advertising practices and the UK's upcoming *Online Safety Bill* (https://bills.parliament.uk/bills/3137#timeline).
73. Model Law for Decentralized Autonomous Organizations (DAOs), COALA (https://coala.global/wp-content/uploads/2021/06/DAO-Model-Law.pdf). For example: decisions at meetings are replaced by proposals raised and automatically put to all tokenholders instantly and transparently on-chain; directors exercising discretion and responsibility are replaced by commonly agreed protocols that a DAO must deterministically execute if certain predefined conditions are met; and service of notices will instead be to the DAO's public blockchain address.
74. Tokens generally do not attach intrinsic rights as it is difficult to give effect to it in the real world, but this is likely to change as the technology matures, e.g., through trait redemption rather than burn-to-redeem.
75. *Ion Science Ltd v Persons Unknown and ors* (unreported, 21 December 2020); *Fetch.ai Ltd and anr v Persons Unknown Category A and ors* [2021] EWHC 2254 (Comm).
76. Ecosystem Readiness: Blockchain Adoption is Driven Externally (https://www.frontiersin.org/articles/10.3389/fbloc.2021.720454/full).

Marcus Bagnall
Tel: +44 7904 809 805 / Email: marcus.bagnall@wiggin.co.uk
Marcus is a leading telecoms and technology specialist. He has spent over a decade advising technology, media and telecoms clients in Europe, Australia and the Middle East. He is well-versed in the intricacies of these industries, and the technical and commercial challenges they face amidst technology evolution. Marcus has a wealth of experience managing complex telecommunications and technology commercial arrangements delivering next-generation networks, digital infrastructure and applying emerging technologies. He has worked on industry-shaping arrangements, including national telecommunications network builds, subsea cable systems, smart city implementation projects and significant technology procurement and outsourcing agreements.

Nicholas Crossland
Tel: +44 20 7927 9619 / Email: nicholas.crossland@wiggin.co.uk
Nicholas is a commercial and regulatory lawyer with a focus on nascent and disruptive technology. He joined Wiggin in 2021 having spent time seconded to two of the world's leading tech companies, providing commercial advice on strategic partnerships in the sector and first-of-their-kind software projects. Nicholas advises one of the world's largest payment providers on regulatory risks from global cross-border crypto services, as well as working with clients across the media and tech sectors on everything from licensing and data flows to AML and commercial issues associated with fintech.

Ben Towell
Tel: +44 7485 383 119 / Email: ben.towell@wiggin.co.uk
Ben is a specialist in telecommunications and internet regulation and focuses on the implications that new technologies pose as disruptors to these areas. Prior to joining Wiggin, Ben was a TMT expert at LexisNexis, researching and producing content across the spectrum.
Ben provides regulatory and commercial advice to many of the world's key players within the telecoms industry, ranging from infrastructure developers to end-user platform providers.

Cecilia Lovell
Tel: +44 7539 904 802 / Email: cecilia.lovell@wiggin.co.uk
Cecilia is a specialist in the telecommunications sector providing advice to key players within the industry on issues of UK and European Union law, competition law and telecommunications law. Cecilia is dual qualified, first completing her LL.B. in Venezuela and further requalifying in Scotland.
Since joining Wiggin, Cecilia's focus has been providing strategic and practical advice to telecoms operators when introducing new services, assessing risk and potential challenges, particularly on the deployment of new technologies such as connected cars, drones, and satellites.

Wiggin LLP

9th Floor, Met Building, 22 Percy Street, London W1T 2BU, United Kingdom
Tel: +44 20 7612 9612 / URL: www.wiggin.co.uk

OFAC sanctions and digital assets: Regulation, compliance, and recent developments

David M. Stetson, Evan T. Abrams, Andrew C. Adams & Sophia Breggia
Steptoe & Johnson LLP

Introduction

In recent years, economic sanctions have become an increasingly important U.S. foreign policy tool and the digital asset industry has become a key focus of sanctions regulators and prosecutors. Regulators and courts have been clear that U.S. economic sanctions laws apply to digital assets, but a number of questions remain regarding the application of economic sanctions to certain digital asset contexts, and the nature of blockchain technology can create complex compliance challenges that are not present in the fiat context.

This chapter provides a high-level background on U.S. economic sanctions generally and then discusses how those sanctions have been applied to digital assets. It also provides a summary of key sanctions enforcement actions in the digital asset industry and discusses compliance expectations and challenges specific to the industry.

OFAC sanctions background

In the United States, the U.S. Department of the Treasury's Office of Foreign Assets Control (OFAC) is the regulatory agency with primary responsibility for implementing U.S. economic sanctions programmes. OFAC is also responsible for civil enforcement while criminal enforcement is conducted by the Department of Justice (DOJ).

U.S. sanctions can be divided into two general categories: primary sanctions; and secondary sanctions. Primary sanctions are applicable to transactions and activities with a U.S. nexus, including transactions and activities occurring in the United States or in which U.S. persons, including individuals and entities, are involved. U.S. secondary sanctions typically apply to conduct undertaken by non-U.S. persons, even if there is no direct U.S. nexus, where the U.S. government has determined that the conduct is counter to a U.S. national security or foreign policy interest.

Primary sanctions

Primary sanctions can apply to specific persons, specific industries or sectors, or to entire countries or regions. The sanctions can also vary in terms of the relevant prohibitions, with some sanctions prohibiting nearly all activity involving the sanctions target and the United States or U.S. persons, wherever located. Other sanctions prohibit a narrower range of conduct, such as certain dealings in debt or equity of the sanctions target.

The United States currently maintains a comprehensive sanctions regime against Cuba, Iran, North Korea, Syria, the Crimea region of Ukraine, and the so-called Donetsk People's Republic (DNR) and Luhansk People's Republic (LNR) regions of Ukraine. U.S. persons are broadly prohibited from dealing with those jurisdictions in any capacity, absent a specific exemption or a licence authorising the conduct in question. Other jurisdictions,

such as Russia and Venezuela, are subject to a broad array of sanctions, but are not subject to the same comprehensive measures applicable to the jurisdictions listed above.[1]

Persons (including entities and individuals) can be targeted by sanctions under a variety of different sanctions programmes and can be identified on a number of lists published by OFAC. The most significant of these lists is the Specially Designated Nationals and Blocked Persons List (SDN List).[2] When a person appears on the SDN List, the property and interests in property of such person must be "blocked" (i.e., frozen) when within the United States or the possession or control of a U.S. person, and U.S. persons are generally prohibited from dealing with specially designated nationals (SDNs). Entities owned 50% or more by one or more SDNs are also considered blocked.

Persons can be added to the SDN List for a broad range of conduct, such as human rights abuses, corruption, nuclear proliferation, engaging in destabilising activity in certain regions, and undermining the democratic nature of certain regimes, among many other activities.

Primary sanctions are a "strict liability" regime, meaning that no knowledge or intent is needed for a civil violation to arise. Criminal violations can arise only from wilful conduct.

Secondary sanctions

Secondary sanctions authorise the imposition of sanctions against persons determined to engage in "sanctionable" conduct. The most common type of secondary sanction is inclusion on the SDN List. However, a range of other sanctions can be imposed. Sanctionable conduct can include a variety of activities; for example, providing material support or goods or services to certain SDNs or "knowingly" engaging in a "significant transaction" for or on behalf of "any person subject to sanctions imposed with respect to the Russian Federation".[3]

OFAC has significant discretion in deciding when to impose secondary sanctions and, generally speaking, is most likely to impose such sanctions where the relevant conduct is both knowing (including having a reason to know) and "material" or "significant" (in certain cases, satisfaction of those elements is a legal requirement for the imposition of secondary sanctions).

OFAC sanctions and digital assets

OFAC guidance indicates that the agency interprets its regulations broadly with regard to digital assets and treats digital assets in largely the same manner as fiat currency. For example, OFAC FAQ 560 states that the OFAC compliance obligations for digital currency transactions and fiat currency transactions are the same, and goes on to explain, "US persons and persons otherwise subject to OFAC jurisdiction, including firms that facilitate or engage in online commerce or process transactions using digital currency, are responsible for ensuring that they do not engage in unauthorized transactions prohibited by OFAC sanctions".[4]

Blocked wallet addresses

OFAC now routinely identifies digital asset wallet addresses as blocked property of SDNs and publishes those wallet addresses in the relevant SDN List entry. Bitcoin wallet addresses form the majority of these wallets, but OFAC has begun identifying wallet addresses associated with a number of other digital assets as well.

Importantly, a wallet address may constitute or contain blocked property regardless of whether it is identified on the SDN List. OFAC's inclusion of an identified wallet in an SDN List entry is intended to assist industry by publicly identifying the wallet address, but any wallet in which an SDN has a property interest must be blocked, regardless of whether the wallet has been identified by OFAC.

Procedures to block crypto assets

OFAC FAQ 646 provides guidance on how persons holding digital assets required to be blocked by OFAC regulations should handle those assets.[5] According to OFAC, an institution may choose, for example, to block each digital currency wallet in which a blocked person has an interest, or may use its own wallet to consolidate wallets that contain the blocked digital currency (similar to an omnibus account), titled, for example, Blocked SDN Digital Currency.[6]

The FAQ adds that each of these methods is satisfactory if there are compliance controls that will allow the digital currency to be unblocked only when the legal prohibition requiring the blocking of the digital currency ceases to apply. The FAQ also explains that holders of blocked digital currency are not obligated to convert the blocked digital currency into traditional fiat currency. Persons holding blocked assets are also required to submit certain reports to OFAC.[7]

OFAC sanctions compliance guidance

In October 2021, OFAC published *Sanctions Compliance Guidance for the Virtual Currency Industry* (VC Compliance Guidance).[8] The guidance reiterates that OFAC rules apply to activity conducted in digital assets, highlights the strict liability nature of OFAC regulations, and summarises the general scope and structure of OFAC sanctions regimes.

The guidance also lays out sanctions compliance best practices for the digital asset industry, which it breaks into five general categories, in keeping the agency's general approach to compliance programmes, including: (1) management commitment; (2) risk assessment; (3) internal controls; (4) testing and auditing; and (5) training.

Among other measures, the guidance highlights the importance of using geolocation tools, such as IP address blocking controls, and conducting appropriate know-your-customer (KYC) due diligence during customer onboarding and throughout the lifecycle of the customer relationship. The guidance also emphasises the value of blockchain transaction monitoring and investigation software and provides non-exhaustive lists of red flags and remedial measures taken by digital asset companies that have been subject to prior OFAC enforcement actions.

OFAC ransomware guidance

On October 1, 2020, OFAC published an *Advisory on Potential Sanctions Risks for Facilitating Ransomware Payments*.[9] A similar, updated version of this advisory was published on September 21, 2021.[10] The advisory notes that OFAC has designated a number of ransomware attackers as SDNs. Other ransomware attackers may not be included on the SDN List but could be located in a jurisdiction subject to comprehensive U.S. sanctions or may be affiliated with the governments of those jurisdictions.

The advisory highlights that OFAC's primary sanctions are a strict liability regime (as discussed above), which can present significant complications for victims of ransomware attacks and those assisting victims, who are often unable to definitively determine the identity of the attacker.

The advisory further notes that companies that facilitate ransomware payments to cyber actors on behalf of victims, including financial institutions, cyber insurance firms, and companies involved in digital forensics and incident response, encourage future ransomware payment demands and also may risk violating OFAC regulations.

The advisory encourages persons to self-report ransomware attacks to appropriate law enforcement agencies. According to OFAC, the agency considers a company's self-initiated and complete report of a ransomware attack to law enforcement or other relevant U.S. government agencies, made as soon as possible after the discovery of an attack, to be a voluntary self-disclosure and a significant mitigating factor in determining an appropriate enforcement response.

Country-specific considerations

Russia

Following Russia's invasion of Ukraine in February 2022, the United States imposed significantly heightened sanctions and export controls measures targeting Russia. The potential use of digital assets by Russia or Russian persons to evade or circumvent those restrictions has been a focal point of U.S. government officials.

For example, Executive Order (EO) 14024, entitled *Blocking Property With Respect To Specified Harmful Foreign Activities of the Government of the Russian Federation*, specifically authorises the SDN designation of persons determined to be responsible for or complicit in "deceptive or structured transactions or dealings to circumvent any United States sanctions, including through the use of digital currencies …" where such action is for or on behalf of, or for the benefit of, directly or indirectly, the Government of the Russian Federation.[11]

OFAC FAQ 1021 further reiterates that the prohibitions imposed on Russia via EO 14024 extend to transactions in virtual currency.[12] The FAQ explains, "Sanctioned Russian persons are known to employ a wide variety of measures in their efforts to evade U.S. and international sanctions. As such, U.S. persons, wherever located, including firms that process virtual currency transactions, must be vigilant against attempts to circumvent OFAC regulations and must take risk-based steps to ensure they do not engage in prohibited transactions".

The FAQ then provides a number of examples of activity involving digital assets that would be prohibited under OFAC rules, such as "virtual currency transactions involving the Central Bank of the Russian Federation, National Wealth Fund of the Russian Federation, or the Ministry of Finance of the Russian Federation", among others.

The FAQ concludes by noting that "OFAC is closely monitoring any efforts to circumvent or violate Russia-related sanctions, including through the use of virtual currency, and is committed to using its broad enforcement authorities to act against violations and to promote compliance".

Venezuelan petro

On March 19, 2018, President Trump issued EO 13827, entitled *Taking Additional Steps to Address the Situation in Venezuela*.[13] The order prohibits "[a]ll transactions related to, provision of financing for, and other dealings in, by a United States person or within the United States, any digital currency, digital coin, or digital token, that was issued by, for, or on behalf of the Government of Venezuela".[14]

The action was specifically aimed at the petro, which is a Venezuelan government-issued digital asset that is purportedly backed by oil and mineral reserves in the country.

However, the order applies more broadly to any other digital assets issued by, for, or on behalf of the government of Venezuela. The action marks the first and only time that OFAC issued a blanket ban on dealings in a given digital asset. However, as more countries, including those subject to comprehensive U.S. sanctions, explore central bank digital currencies (CBDCs) or other types of government-backed digital assets, it is possible that OFAC will take additional, similar actions in the future.

OFAC enforcement actions against digital asset platforms

Beginning in December 2020, with an enforcement action against BitGo,[15] OFAC has brought a series of enforcement actions against digital asset platforms. In addition to BitGo, the targeted companies include BitPay, Bittrex,[16] Kraken, and Poloniex.[17] While each enforcement action was factually unique, all of them involved the use of the platform by users located in comprehensively sanctioned jurisdictions including Cuba, Iran, Sudan, Syria, and the Crimea region of Ukraine. In a number of cases, OFAC found that the platforms had reason to know of the location of the users based on either KYC documents or geolocation data associated with a user's IP address used to access the platform.

Among other takeaways, the actions demonstrate the importance of using all available risk-relevant data to assist in sanctions compliance and taking measures to prevent users located in comprehensively sanctioned jurisdictions from accessing the platforms.

SDN designation of non-U.S. exchanges, mixers, and tumblers

Starting in late 2021, OFAC began a string of SDN designations focused on non-U.S. digital asset exchanges, mixers, and tumblers. The targeted platforms include SUEX, Chatex, Garantex, Blender.io, and Hydra Market.[18] All of those platforms were designated pursuant to EO 13694, *Blocking the Property of Certain Persons Engaging in Significant Malicious Cyber-Enabled Activities*.[19]

These actions highlight the significant discretion of OFAC to target actors that it believes are acting contrary to U.S. foreign policy or national security objectives, regardless of the jurisdiction of those actors and regardless of whether there is any U.S. nexus.

The SDN designations have implications both for U.S. persons and persons acting within the United States, who are generally prohibited from dealing with SDNs, and for non-U.S. persons outside the United States. Most EOs authorising the issuance of SDN designations, including EO 13694, also authorise OFAC to designate any person determined to have "materially assisted, sponsored, or provided financial, material, or technological support for, or goods or services in support of … any person whose property and interests in property are blocked pursuant to this order".[20] In other words, persons who deal with SDNs also risk being designated as SDNs themselves. Therefore, any person dealing with an SDN digital asset platform may face sanctions risk from OFAC.

Tornado Cash and implications for DeFi platforms

Perhaps the most contentious and widely followed OFAC action in the digital asset space has been its designation of Tornado Cash as an SDN.[21]

OFAC designated Tornado Cash in 2022 under EO 13694, as amended, and EO 13722,[22] which pertains to North Korea. OFAC cited the use of Tornado Cash by the Lazarus Group, a North Korean state-sponsored hacking group, to launder hundreds of millions of dollars for the benefit of North Korea as the primary reason for the designation.[23]

When designating Tornado Cash, OFAC determined that Tornado Cash was a "person" that was eligible for designation under the relevant authorities. OFAC also identified the smart contracts underpinning the Tornado Cash protocol as property in which Tornado Cash has a "property interest" (i.e., OFAC concluded that the smart contracts were blocked property). Those findings were challenged in *Joseph Van Loon, et al. v. Department of Treasury, et al.*[24] and ultimately upheld by the district court.

The *Van Loon* decision

The district court in *Van Loon* found that Tornado Cash was a "person", which is defined in the relevant EOs to include "entities" and, in particular, "associations". While the term "association" is not defined in the EOs or elsewhere in applicable OFAC rules, the court defined an association as "[a] body of persons who have combined to execute common purpose or advance a common cause".[25] The court explained that the Tornado Cash "association" is "composed of its founders, its developers, and its [decentralised autonomous organisation, or] DAO".[26]

The court then explained that the underlying smart contracts were "property" in which the association had an interest (and, therefore, were subject to blocking pursuant to OFAC rules). The court first noted that "property" is broadly defined in existing OFAC rules to include a wide range of items, including "contracts of any nature whatsoever" and "services of any nature whatsoever".[27] It found that the smart contracts were "contracts", and even if some of the underlying code could not be accurately described as a contract, "Tornado Cash promoted and advertised the contracts and its abilities and published the code with the intention of people using it—hallmarks of a unilateral offer to provide services".[28]

The court also found that the association had an "interest" in this property, pointing to OFAC's broad regulatory definition of "interest" as "an interest of any nature whatsoever, direct or indirect".[29] It explained, "Tornado Cash has a beneficial interest in the deployed smart contracts because they provide Tornado Cash with a means to control and use crypto assets. The smart contracts generate fees in the form of TORN tokens for the DAO when users execute a relayer-facilitated transaction".[30]

It is worth noting that, at the time of this writing, the district court decision is being appealed and a separate action brought by Coin Center is continuing to be litigated in another federal court in Florida. Therefore, the *Van Loon* decision may not be the last word on this matter in U.S. courts. Nonetheless, it marks a significant victory for OFAC and a decision to which the decentralised finance (DeFi) industry must pay careful attention.

The *Van Loon* decision did not find that OFAC could designate the underlying code itself, but rather that OFAC did and could designate an "association" of individuals connected to an underlying protocol or software and who have a "property interest" in that code, or at a minimum, in transactions that are executed by that code.

The ruling, unless reversed, indicates that OFAC can designate any DeFi platform that it determines has engaged in sanctionable conduct, so long as the platform is developed, operated, or governed by an "association" of persons engaged in a "common purpose" or is otherwise able to be construed as an "entity", as defined under applicable OFAC regulations. That holding is likely to apply to a broad array of DeFi platforms currently in operation.

The *Van Loon* court also relied heavily on the specific facts of Tornado Cash, which may not necessarily be present in all cases. For example, it is unclear how the court's ruling would apply to a situation where a developer wrote code, published it on GitHub (or another platform) for free public use, and then walked away with no further involvement, management, or financial stake in how the code operates or executes transactions. Similarly, it is unclear whether the court would have reached the same conclusion if there had been no DAO and no financial benefit flowing to the DAO from the execution of relayer-facilitated transactions. Therefore, *Van Loon* may not necessarily apply to all decentralised blockchain protocols, particularly those with facts that are significantly different from Tornado Cash.

Nonetheless, because many, if not most, DeFi projects have some level of ongoing involvement from the founders, a DAO, or otherwise, the *Van Loon* ruling is likely to have significant implications for those platforms.

Designation of Tornado Cash founder and DOJ indictment

Shortly after the *Van Loon* ruling, OFAC announced the SDN designation of Roman Semenov, one of three alleged co-founders of Tornado Cash,[31] and DOJ charged Semenov and Roman Storm, another Tornado Cash founder, with multiple alleged criminal violations related to anti-money laundering (AML) and economic sanctions laws.[32] Semenov and Storm allegedly coded Tornado Cash, held a significant number of governance tokens, and developed a frontend user interface, over which both individuals retained control, that helped users access the protocol. Users were not required to access the protocol via this frontend user interface, but, according to the indictment, the significant majority of users did use the interface.

The indictment alleges that the defendants were aware that the Tornado Cash protocol was being used by a number of bad actors to launder the proceeds of hacks and other illegal conduct. It also alleges that the defendants profited from such activity through their holding of TORN tokens (the governance token of the Tornado Cash DAO) and the implementation of a "relayer register" that required Tornado Cash relayers to purchase TORN tokens in order to be chosen to process withdrawals from the Tornado Cash frontend user interface.

The indictment further alleges that the founders made changes to the frontend user interface to prevent transactions flowing directly from wallets that had been identified as blocked property of the Lazarus Group (and others), but privately acknowledged that the measures were inadequate because they could easily be bypassed by transferring tokens from the identified wallets into a new wallet and then using the Tornado Cash frontend.

Storm and Semenov were charged with three counts, including (1) conspiracy to commit money laundering, (2) conspiracy to operate an unlicensed money-transmitting business, and (3) conspiracy to violate the International Emergency Economic Powers Act (IEEPA).[33] Given the sanctions focus of this chapter, we focus on the third count related to IEEPA (although the first two counts raise a number of important considerations with respect to AML laws in the DeFi context).

Assuming that the Lazarus Group did in fact use the frontend user interface and the defendants had knowledge of this, the violations of IEEPA appear relatively straightforward. The defendants maintained a website that assisted users in engaging in financial transactions via the underlying Tornado Cash protocol and were aware that an SDN was using the services provided by the website. With that said, the breadth of the indictment's allegations is striking; the IEEPA allegations relate not only to the defendant's activities in offering the frontend user interface, but to the defendants' roles as founders and designers of, and ongoing involvement with, the underlying protocol and their allegedly wilful inaction in the face of ongoing sanctioned transactions flowing through Tornado Cash. The indictment alleges that the defendants not only had control over the user interface, but also exercised at least some degree of control over the underlying protocol, including the continued ability to profit from its operation. The indictment does not provide insight into how DOJ might view a situation without a user interface and involving a fully decentralised protocol over which no person was able to exercise any degree of control.

The indictment highlights the importance of founders and developers considering economic sanctions compliance at the design, build, and operational stages of any new DeFi projects. It also highlights the need to take action when a founder or developer becomes aware that a project may be used by sanctioned parties and for that action to be meaningful. The indictment identifies "KYC procedures, transaction monitoring, [and] blockchain tracing" as other measures that Storm and Semenov could have taken.[34]

Digital assets and export controls

While this chapter is focused principally on economic sanctions, it makes sense to briefly address the closely related area of export controls. Particularly since the Russian invasion of Ukraine in February 2022, the U.S. government has become increasingly focused on the potential role of financial institutions and others involved in international payments in identifying and reporting potential export controls violations. For example, the Department of Commerce's Bureau of Industry and Security and the Department of the Treasury's Financial Crimes Enforcement Network (FinCEN) have issued joint alerts urging financial institutions to exercise "increased vigilance" with respect to potential Russia and Belarus export controls evasion attempts.[35]

In terms of enforcement, on October 19, 2022, DOJ charged five Russian nationals and two Venezuelan nationals with using a complex series of transactions involving digital assets and shell companies to unlawfully obtain U.S. military technology and sanctioned Venezuelan oil.[36]

As U.S. export controls continue to expand and increase in complexity, this trend is likely to continue and digital asset platforms should consider export controls compliance in addition to OFAC sanctions.

Compliance programme considerations

OFAC regulations do not technically require any entity to implement an OFAC compliance programme. However, because of the strict liability standard under U.S. primary sanctions and OFAC's broad discretion with respect to secondary sanctions, many entities elect to implement a robust sanctions compliance programme.[37] Moreover, many digital currency projects operating in the United States are subject to the AML and KYC requirements of the Bank Secrecy Act (BSA), whether as money services businesses or as certain Securities and Exchange Commission (SEC) or Commodity Futures Trading Commission (CFTC) registrants. These BSA obligations, in turn, effectively impose sanctions screening as a part of an effective compliance programme.

OFAC and DOJ, which enforces criminal sanctions penalties, have made clear in a number of instances that maintaining a compliance programme is an important factor when they determine whether to bring an enforcement action and what penalty to impose. For example, OFAC's *Economic Sanctions Enforcement Guidelines*, which set out general parameters regarding how OFAC approaches enforcement in the event of a violation of OFAC regulations, include maintenance of a compliance programme as one of the general factors affecting OFAC's enforcement response to an apparent violation.[38] Specifically, the agency will consider – as either a mitigating factor or an aggravating factor – the existence, nature, and adequacy of a person's risk-based OFAC compliance programme at the time of the apparent violation.

OFAC has also issued guidance entitled *A Framework for Compliance Commitments*, which outlines the key elements OFAC expects to see when reviewing an entity's compliance programme.[39] It also cites the lack of a formal OFAC sanctions compliance programme as a primary root cause of OFAC sanctions violations and notes that OFAC frequently cites the absence of such a programme as an aggravating factor in its enforcement analysis.

With respect to criminal enforcement, DOJ publishes a reference guide for prosecutors known as the *Justice Manual*, which includes a section on Principles of Federal Prosecution of Business Organizations that outlines various factors that federal prosecutors consider

when taking action against a business. One of those factors is the adequacy and effectiveness of the entity's compliance programme at the time of the offence. The manual explains, "the critical factors in evaluating any program are whether the program is adequately designed for maximum effectiveness in preventing and detecting wrongdoing by employees and whether corporate management is enforcing the program or is tacitly encouraging or pressuring employees to engage in misconduct to achieve business objectives".[40] Moreover, the recently revised National Security Division (NSD) Enforcement Policy for Business Organizations, published on March 1 of this year, reiterates the importance of a demonstrated commitment to maintaining an effective compliance programme specifically in the context of evaluating remedial efforts in the face of sanctions violations.

OFAC's VC Compliance Guidance, discussed above, also notes that all companies in the digital asset industry are encouraged to develop, implement, and routinely update a tailored, risk-based sanctions compliance programme.

Digital asset-specific compliance programme considerations

In addition to the above general sanctions compliance considerations, there are several sanctions considerations that are unique to digital asset companies. The use of blockchain analytics is a particularly important tool for the industry, and the ability to trace many digital asset transactions on public blockchains can provide detailed insight into the transactions of a given wallet, including any links to known bad actors or sanctioned persons.

Many blockchain analytics service providers offer services that can help identify whether a given wallet is specifically included on the SDN List, is associated with an SDN, or has otherwise interacted with a wallet known to belong to a sanctioned person. For privacy-enhanced blockchains with more limited information publicly available on the blockchain, companies should consider whether alternative means exist to mitigate the potentially heightened sanctions compliance risk of these blockchains and whether using these blockchains falls within their risk tolerance.

Both OFAC's enforcement actions and its sanctions compliance guidance highlight the importance of geolocating a user's IP address to identify whether a user is accessing a digital asset platform from a device located in a comprehensively sanctioned jurisdiction. While sophisticated users can obscure their IP address by using a VPN or through other means, many users do not take these measures, as evidenced by OFAC's enforcement actions.

As noted above, OFAC has issued specific guidance on blocking digital assets. Digital asset companies should familiarise themselves with this guidance and consider creating written procedures for how the company will handle blocked assets, which may include procedures for periodic testing to ensure that compliance controls deployed to block digital assets are functioning properly.

There are additional and significant challenges that come with implementing compliance measures in a decentralised context, including identifying who is responsible for determining and implementing the appropriate measures and how to achieve compliance objectives while maintaining the decentralised nature of the protocol. These challenges are heightened by the fact that the movement toward greater centralisation can have important implications under other legal regimes, such as securities law and even the AML rules of certain jurisdictions that do not extend to fully decentralised platforms.

Open questions and enforcement outlook

While OFAC has noted that compliance obligations for transactions involving digital assets are the same as for fiat currency transactions, there are still many open questions with

respect to how OFAC views the application of its regulations to the digital asset space. For example, the agency has not issued any formal guidance on how it views the obligations of persons such as:

- crypto miners and other validators;
- coders and developers;
- governance token holders in DeFi projects; and
- persons serving in foundations associated with specific blockchains.

In many of these instances, participants may have limited or no visibility into persons with whom they are directly or indirectly dealing or have no ability to limit the group of users with whom they directly or indirectly interact. For example, a miner validating a block in a blockchain typically has no ability to limit the transactions in that block and only limited insight into the parties to the transactions in the block.

There are also significant questions regarding the obligations of developers and coders that create and release protocols. The indictment of Tornado Cash's founders, discussed above, provides some insight into how DOJ views the compliance obligations of such persons. However, given a number of the unique facts in that case, it is unclear how broadly the lessons from that indictment can be applied.

While the industry continues to wait for additional guidance and clarity on some of these questions, it seems likely that OFAC SDN designations and enforcement actions both from OFAC and DOJ will continue and, perhaps, increase.

Recent organisational and personnel changes within DOJ point toward increased focus on the nexus between financial crimes, including those conducted in digital assets, and sanctions violations. Such prosecutions can require expertise from a number of areas within DOJ, including the NSD, the Money Laundering and Asset Recovery Section, and the criminal division and money laundering units of the various U.S. attorneys' offices. A number of DOJ initiatives, including Task Force KleptoCapture, the National Cryptocurrency Enforcement Team, and the recent appointments of a Chief Corporate Enforcement counsel and Deputy Corporate Enforcement counsel within NSD, are intended to enhance cooperation and expertise across the Department and may lead to additional prosecutions involving digital assets and sanctions going forward.

* * *

Endnotes

1. *See* U.S. Dep't Treas. Off. Foreign Assets Control, Sanctions Programs and Country Information, available at https://ofac.treasury.gov/sanctions-programs-and-country-information
2. *See* U.S. Dep't Treas. Off. Foreign Assets Control, Specially Designated Nationals and Blocked Persons List (SDN List), available at https://ofac.treasury.gov/specially-designated-nationals-and-blocked-persons-list-sdn-human-readable-lists
3. 22 U.S.C. § 8909; *see* Countering America's Adversaries Through Sanctions Act (CAATSA), Pub. L. No. 115-44 (Aug. 2, 2017).
4. U.S. Dep't Treas. Off. Foreign Assets Control, Questions on Virtual Currency: FAQ 560, available at https://ofac.treasury.gov/faqs/560#:~:text=Are%20my%20OFAC%20compliance%20obligations,currency%20or%20traditional%20fiat%20currency%3F&text=Yes%2C%20the%20obligations%20are%20the%20same

5. *See* U.S. Dep't Treas. Off. Foreign Assets Control, Questions on Virtual Currency: FAQ 646, available at https://ofac.treasury.gov/faqs/646
6. *See id*.
7. 31 C.F.R. § 501.603.
8. U.S. Dep't Treas. Off. Foreign Assets Control, *Sanctions Compliance Guidance for the Virtual Asset Industry* (Oct. 2021), available at https://ofac.treasury.gov/media/913571/download?inline
9. Ransomware typically involves a hacker breaching a company's IT infrastructure and encrypting a company's data or other systems. The attacker then typically demands that the victim pay a ransom in exchange for a decryption key that allows the victim to unlock the IT systems or data. The ransom is almost always demanded in cryptocurrency.
10. U.S. Dep't Treas. Off. Foreign Assets Control, *Updated Advisory on Potential Sanctions Risks for Facilitating Ransomware Payments* (Sept. 21, 2021), available at https://ofac.treasury.gov/media/912981/download?inline
11. Exec. Order No. 14024, 86 Fed. Reg. 20249 (Apr. 19, 2021).
12. *See* U.S. Dep't Treas. Off. Foreign Assets Control, Russian Harmful Foreign Activities Sanctions: FAQ 1021, available at https://ofac.treasury.gov/faqs/1021
13. Exec. Order No. 13827, 83 Fed. Reg. 12469 (Mar. 19, 2018).
14. *Id.*
15. *See* Enforcement Release, U.S. Dep't Treas. Off. Foreign Assets Control, OFAC Enters Into $98,830 Settlement with BitGo, Inc. for Apparent Violations of Multiple Sanctions Programs Related to Digital Currency Transactions (Dec. 30, 2020), available at https://ofac.treasury.gov/media/50266/download?inline
16. The case against Bittrex involved a joint action between OFAC and the U.S. Department of the Treasury's Financial Crimes Enforcement Network (FinCEN), which issued a consent decree regarding alleged violations of the Bank Secrecy Act (BSA) and its implementing regulations, in addition to the sanctions violations identified by OFAC.
17. *See* Enforcement Release, U.S. Dep't Treas. Off. Foreign Assets Control, OFAC Enters Into $507,375 Settlement with BitPay, Inc. for Apparent Violations of Multiple Sanctions Programs Related to Digital Currency Transactions (Feb. 18, 2021), available at https://ofac.treasury.gov/media/54341/download?inline; Enforcement Release, U.S. Dep't Treas. Off. Foreign Assets Control, OFAC Settles with Bittrex, Inc. for $24,280,829.20 Related to Apparent Violations of Multiple Sanctions Programs (Oct. 11, 2022), available at https://ofac.treasury.gov/media/928746/download?inline; Enforcement Release, U.S. Dep't Treas. Off. Foreign Assets Control, OFAC Settles with Virtual Currency Exchange Kraken for $362,158.70 Related to Apparent Violations of the Iranian Transactions and Sanctions Regulations (Nov. 28, 2022), available at https://ofac.treasury.gov/media/929541/download?inline; Enforcement Release, U.S. Dep't Treas. Off. Foreign Assets Control, OFAC Settles with Poloniex, LLC for $7,591,630 Related to Apparent Violations of Multiple Sanctions Programs (May 1, 2023), available at https://ofac.treasury.gov/media/931701/download?inline
18. *See* Press Release, U.S. Dep't Treas. Off. Foreign Assets Control, Treasury Takes Robust Actions to Counter Ransomware (Sept. 21, 2021), available at https://home.treasury.gov/news/press-releases/jy0364; Press Release, U.S. Dep't Treas. Off. Foreign Assets Control, Treasury Continues to Counter Ransomware as Part of Whole-of-Government Effort; Sanctions Ransomware Operators and Virtual Currency

Exchange (Nov. 8, 2021), available at https://home.treasury.gov/news/press-releases/jy0471#:~:text=Suex%20was%20sanctioned%20on%20September,posed%20by%20criminal%20ransomware%20actors; Press Release, U.S. Dep't Treas. Off. Foreign Assets Control, Treasury Sanctions Russia-Based Hydra, World's Largest Darknet Market, and Ransomware-Enabling Virtual Currency Exchange Garantex (Apr. 5, 2022), available at https://home.treasury.gov/news/press-releases/jy0701; Press Release, U.S. Dep't Treas. Off. Foreign Assets Control, U.S. Treasury Issues First-Ever Sanctions on a Virtual Currency Mixer, Targets DPRK Cyber Threats (May 6, 2022), available at https://home.treasury.gov/news/press-releases/jy0768

19. Exec. Order No. 13694, 80 Fed. Reg. 18077 (Apr. 2, 2015).
20. *Id.*
21. *See* Press Release, U.S. Dep't Treas. Off. Foreign Assets Control, U.S. Treasury Sanctions Notorious Virtual Currency Mixer Tornado Cash (Aug. 8, 2022), available at https://home.treasury.gov/news/press-releases/jy0916
22. Exec. Order No. 13722, 82 Fed. Reg. 17331 (Apr. 10, 2017).
23. *See* Press Release, U.S. Dep't Treas. Off. Foreign Assets Control, U.S. Treasury Sanctions Notorious Virtual Currency Mixer Tornado Cash (Aug. 8, 2022), available at https://home.treasury.gov/news/press-releases/jy0916
24. *See* Order, *Van Loon v. Dep't Treas.*, No. 23-cv-312-RP (W.D. Tex. Aug. 17, 2023).
25. *Id.* at 14.
26. *Id.* at 15.
27. *Id.* at 17.
28. *Id.* at 18.
29. *Id.* at 19.
30. *Id.*
31. *See* Press Release, U.S. Dep't Treas. Off. Foreign Assets Control, Treasury Designates Roman Semenov, Co-Founder of Sanctioned Virtual Currency Mixer Tornado Cash (Aug. 23, 2023), available at https://home.treasury.gov/news/press-releases/jy1702
32. *See U.S. v. Storm*, No. 23-cr-430 (S.D.N.Y. Aug. 23, 2023).
33. *See* 50 U.S.C. ch. 35 § 1701 *et seq.* IEEPA is the federal statute underpinning the SDN designation of the Lazarus Group.
34. *See U.S. v. Storm*, No. 23-cr-430 (S.D.N.Y. Aug. 23, 2023).
35. *See* Joint Alert, Fin. Crimes Enf't Network & Bureau Indus., Fin-2022-Alert003, FinCEN and the U.S. Department of Commerce's Bureau of Industry and Security Urge Increased Vigilance for Potential Russian and Belarusian Export Control Evasion Attempts (Jun. 28, 2022), available at https://www.fincen.gov/sites/default/files/2022-06/FinCEN%20and%20Bis%20Joint%20Alert%20FINAL.pdf; Joint Alert, Fin. Crimes Enf't Network & Bureau Indus., FIN-2-23-Alert004, Supplemental Alert: FinCEN and the U.S. Department of Commerce's Bureau of Industry and Security Urge Continued Vigilance for Potential Russian Export Control Evasion Attempts (May 19, 2023), available at https://www.fincen.gov/sites/default/files/shared/FinCEN%20and%20BIS%20Joint%20Alert%20_FINAL_508C.pdf
36. *See* Press Release, U.S. Dep't J., Five Russian Nationals and Two Oil Traders Charged in Global Sanctions Evasion and Money Laundering Scheme (Oct. 19, 2022), available at https://www.justice.gov/usao-edny/pr/five-russian-nationals-and-two-oil-traders-charged-global-sanctions-evasion-and-money
37. Some entities, such as U.S. financial institutions, may also be required or expected to have an OFAC compliance programme under other applicable regulatory regimes.

38. 31 C.F.R. pt. 501, App. A.
39. *See* U.S. Dep't Treas. Off. Foreign Assets Control, A Framework for OFAC Compliance Commitments (2019), available at https://ofac.treasury.gov/media/16331/download?inline
40. *Justice Manual*, 9-28.800, 2019 WL 5864449, at *1. Judges also take into account an effective compliance and ethics programme when determining appropriate sentencing under the U.S. Sentencing Commission's Sentencing Guidelines (U.S.S.G. 8B2.1).

David M. Stetson
Tel: +1 212 378 7521 / Email: dstetson@steptoe.com

David Stetson, a former senior lawyer at the U.S. Department of the Treasury, Office of Foreign Assets Control (OFAC) and former global co-head of sanctions compliance at Goldman Sachs, leads investigations and advises clients on OFAC sanctions and related anti-money laundering (AML) and export controls issues. Drawing on his government and in-house experience, he focuses on helping clients apply rapidly evolving sanctions requirements across a broad range of financial products and services, including investment banking, securities trading, commercial lending, merchant banking, commodities trading, asset management, and consumer banking.

Evan T. Abrams
Tel: +1 202 429 3052 / Email: eabrams@steptoe.com

Evan Abrams counsels financial institutions, multinational corporations, and individuals on a variety of international regulatory and compliance matters. He regularly advises clients on issues related to anti-money laundering (AML), economic sanctions, export controls, foreign anti-corruption, the Committee on Foreign Investment in the United States (CFIUS), and the Defense Counterintelligence and Security Agency (DCSA). Among other sectors, his practice focuses on emerging technology, including financial technology (FinTech), where he leverages his deep understanding of business trends and technological developments to help clients achieve their commercial objectives while complying with complex regulatory regimes.

Andrew C. Adams
Tel: +1 212 957 3081 / Email: acadams@steptoe.com

Andrew Adams advises in the areas of government and internal investigations, corporate governance, and white-collar and regulatory matters. His practice focuses on anti-money laundering compliance, U.S. economic countermeasures, and national security crisis response, drawing on his time as the inaugural Director of the Department of Justice's Task Force KleptoCapture, a multi-agency response group focused on the economic sanctions and export controls imposed in response to Russia's invasion of Ukraine, and on his service as acting Deputy Assistant Attorney General for the National Security Division of the Department of Justice, with oversight of the Division's sanctions, export control, and national security cyber investigations.

Sophia Breggia
Tel: +1 202 429 3028 / Email: sbreggia@steptoe.com

Sophia Breggia counsels clients on a range of regulatory and legislative matters in the financial services sector, including those before the Commodity Futures Trading Commission (CFTC), the Securities and Exchange Commission (SEC), the Department of the Treasury, the Federal Reserve, and the Consumer Financial Protection Bureau (CFPB). Her practice involves advising financial institutions, private FinTech companies, and public companies engaged in the blockchain and cryptocurrency space on compliance with federal law and regulation. Sophia also has experience representing clients in investigations before the Department of Justice (DOJ), the SEC, and the CFTC.

Steptoe & Johnson LLP

1330 Connecticut Avenue, NW, Washington, D.C. 20036, USA
Tel: +1 202 429 3000 / URL: www.steptoe.com

False friends and creditors: The saga of recent crypto insolvencies

Stephen Rutenberg, David Brill & Michael DiPietro
Polsinelli

"How did you go bankrupt?" Bill asked.
"Two ways", Mike said. "Gradually and then suddenly."
"What brought it on?"
"Friends", said Mike. "I had a lot of friends. False friends. Then I had creditors, too. Probably had more creditors than anybody in England."

Ernest Hemingway
The Sun Also Rises

Introduction

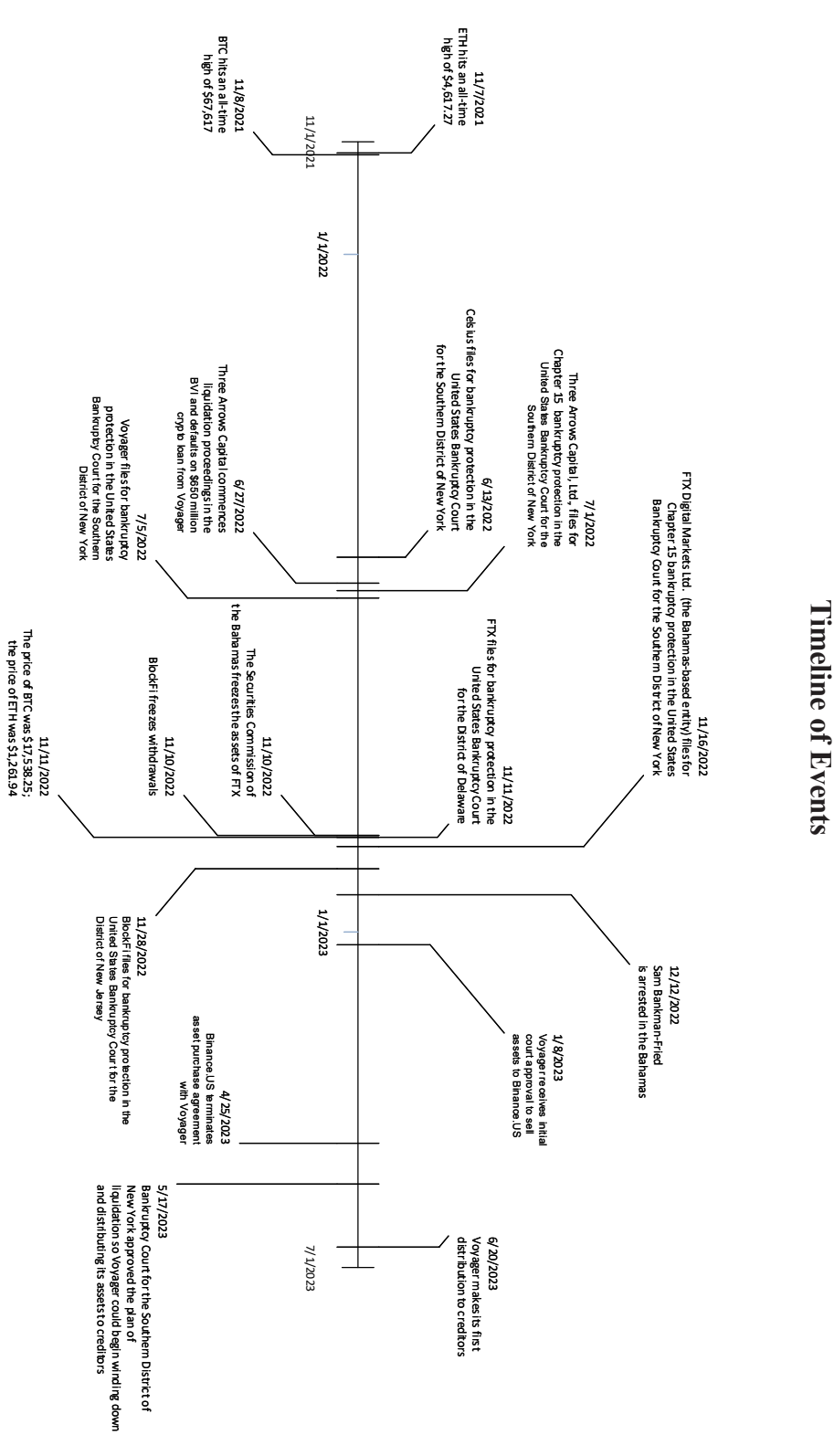
In 2021, it was all crypto everywhere, or so it appeared, with headlines ranging from Miami's mayor proudly dubbing the city the "crypto capital" to entire nations embracing Bitcoin as a legitimate currency. The art world was also ablaze with excitement over Non-Fungible Tokens (NFTs). Su Zhu, a founder of the now-defunct Three Arrows Capital (3AC), encapsulated the pervasive enthusiasm and warned: "If you don't understand crypto and refuse to learn, it's gonna be a tough century for you."

However, 2022 and 2023 ushered in a starkly different reality. Major crypto-related companies collapsed, leaving customers and investors reeling from billions in losses. This downturn was particularly painful because many of these losses were incurred in ways consumers had not anticipated.

The catalyst for these collapses did not arise from inherent flaws in blockchain technology, a waning public interest, or even excessive governmental regulations. Instead, they were precipitated by questionable relationships between these crypto enterprises and the utilisation – or possible misutilisation – of credit. The haunting echoes of Hemingway's "false friends and creditors" reverberated through the unfolding events.

This chapter explores the downfall of significant figures in the crypto sphere, including Voyager Digital Holdings, Inc. (Voyager), Celsius Network (Celsius), 3AC, BlockFi, and FTX, all of which collapsed in 2022, with their cases continuing to be restructured throughout 2023. Notably, 3AC, a significant investor in crypto ventures, found itself both a lender and borrower within the crypto ecosystem. Voyager, Celsius, and BlockFi were involved in providing loans backed by crypto assets or offering returns to depositors who lent their crypto. Meanwhile, FTX operated as a crypto exchange, facilitating the buying and selling of crypto assets. What remained concealed from many FTX users was the platform's purported involvement in various investments and loans using the assets held on its exchange.

In many respects, these entities and their misfortunes were intricately linked. For instance, Voyager's downfall was intertwined with 3AC's inability to repay a $650 million crypto loan.


Timeline of Events
11/16/2022
FTX Digital Markets Ltd. (the Bahamas-based entity) files for Chapter 15 bankruptcy protection in the United States Bankruptcy Court for the Southern District of New York
12/12/2022
Sam Bankman-Fried is arrested in the Bahamas
1/8/2023
Voyage receives initial court approval to sell assets to Binance.US
4/25/2023
Binance.US terminates asset purchase agreement with Voyager
5/17/2023
Bankruptcy Court for the Southern District of New York approved the plan of liquidation so Voyager could begin winding down and distributing its assets to creditors
6/20/2023
Voyager makes its first distribution to creditors
7/1/2023
1/1/2023
11/28/2022
BlockFi files for bankruptcy protection in the United States Bankruptcy Court for the District of New Jersey
11/11/2022
The price of BTC was $17,538.25; the price of ETH was $1,261.94
11/10/2022
BlockFi freezes withdrawals
11/10/2022
The Securities Commission of the Bahamas freezes the assets of FTX
11/11/2022
FTX files for bankruptcy protection in the United States Bankruptcy Court for the District of Delaware
7/5/2022
Voyager files for bankruptcy protection in the United States Bankruptcy Court for the Southern District of New York
6/27/2022
Three Arrows Capital commences liquidation proceedings in the BVI and defaults on $650 million crypto loan from Voyager
6/13/2022
Celsius files for bankruptcy protection in the United States Bankruptcy Court for the Southern District of New York
7/1/2022
Three Arrows Capital, Ltd., files for Chapter 15 bankruptcy protection in the United States Bankruptcy Court for the Southern District of New York
1/1/2022
11/1/2021
11/8/2021
BTC hits an all-time high of $67,617
11/7/2021
ETH hits an all-time high of $4,617.27

Simultaneously, BlockFi's downfall stemmed from approximately $1 billion locked up or lost within FTX or its affiliated trading entities. Having delved into the background and current status of these cases, we will further explore the intriguing aftermath, including the impact on the U.S. Bankruptcy Code due to the unique nature of these cases and the valuable lessons to be gleaned from these tumultuous events.

3AC

Founded in 2012 by Ivy League-educated Su Zhu and Kyle Davies, at its peak with more than $10 billion under management, 3AC was considered one of the more adult or reputable companies in the emerging blockchain industry. Although 3AC was based in the British Virgin Islands (BVI), it appears to have conducted most of its business out of Singapore and had U.S. operations.

A company willing to bet on innovative technology and first-time founders, it was a lead investor in start-up crypto projects, second only to the ubiquitous Andreessen Horowitz. Su Zhu embraced an extremely optimistic philosophy or theory. The theory presupposed that prices would increase for the foreseeable future due to the rapidly expanding adoption of cryptocurrency and that cryptocurrency would avoid the standard cycles in finance. This he called a "Supercycle". With this philosophy in mind, the founders of 3AC optimistically bet on many projects and possibly did not give enough attention to risk management. However, what likely brought down 3AC and caused a cascade of other failures was that 3AC borrowed billions of dollars from other companies in the crypto space, which it used to make investments. Most other venture funds are primarily funded by investor capital. As such, when several investments failed, including the now-defunct stablecoin, Terra, 3AC was unable to repay its loans and was forced to file for liquidation in the BVI.

On June 27, 2022, Russell Crumpler and Christopher Farmer were appointed as Joint Liquidators in the BVI. The Joint Liquidators were tasked with finding and selling the assets of 3AC and using the proceeds to pay back creditors. Compared to the U.S. bankruptcy process, the liquidation in the BVI is an opaque process. It is more focused on creditor recoveries, rather than allowing the debtor an attempt to restructure. While there is a committee of creditors, it does not have the same, formalised power as the unsecured creditors' committees of the U.S. bankruptcy system. Since the Joint Liquidators' appointment, little progress has been made on reclaiming assets. Among the issues the Joint Liquidators are facing is the refusal of the founders of 3AC to reliably cooperate in the administration of the liquidation process. The BVI liquidation process seems, at least in the case of 3AC, to be moving slower than similar cases being administered under the structure of the U.S. Bankruptcy Code. However, the fees and expenses of the Joint Liquidators are likely much less than those of their U.S. counterparts.

Celsius

Crypto lender Celsius was founded in 2017 by Alex Mashinsky to attempt to solve the issues faced by crypto holders. The first issue was that BTC, and to a great extent, ETH, did not pay interest. Holders of BTC were looking for a way to make money off of the BTC they were holding, rather than simply relying on the crypto to increase in value. The second issue was that many holders of crypto assets wanted to obtain funds for their crypto without having to sell it. Celsius solved both of these issues in a way that appeared too good to be true, and in the end, it was. Under Celsius' "Earn" programme, parties were offered an interest rate of up to 10% for depositing crypto and giving Celsius the right to invest it. Not all lenders understood or were made aware that they were losing the title to their BTC. Under the separate "Borrower" programme, people could borrow against their crypto at an often exceptionally low or zero interest rate. Unlike a bank that charges a borrower a

higher interest rate than it pays its depositors, Celsius was doing the opposite. To fund this operation, they made other loans, including to 3AC, and traded crypto. Celsius also financed itself through an initial token offering of its own native cryptocurrency – the CEL token.

On June 12, 2022, Celsius announced that it was "pausing" all withdrawals from its accounts, including Earn accounts. Many holders had considered Celsius the equivalent of a bank and deposited their life's savings there. Celsius blamed market conditions for this pause on withdrawals. Soon, it became clear that Celsius did not have adequate crypto reserves to pay back its holders. On July 13, 2022, Celsius filed for bankruptcy protection in the Southern District of New York.

The most contentious issue, in this case, is that many creditors, particularly in the Earn programme, deposited their crypto with the expectation that they would be able to withdraw it at will and that the deposited crypto would be considered their property – not property of Celsius' estate against which they only have an unsecured claim. However, for several reasons, one being that almost all the Earn creditors agreed to terms and conditions stating that they were giving up title to their deposited crypto, the Court ruled that the contracts entered into by the Earn creditors were valid and enforceable. The Court did permit the creditors to enter separate claims for fraud, which many of them did.

Another critical issue with the case was how holders of the CEL token issued by Celsius would be treated. Should these holders be given a claim in the case like that of the Earn holders, or should their interest be considered more akin to equity?

Given the fraud allegations made by a number of creditors and other stakeholders, the Court appointed Shoba Pillay of the law firm of Jenner & Block LLP as an examiner to investigate the allegations and other matters. On January 31, 2023, she issued her report, which was critical of the company's founder and former management. Pillay accused them of misleading customers and running something approaching a Ponzi scheme by using customer funds to purchase CEL tokens to support its price, thus benefitting insiders with vast CEL holdings.

A big debate in the Celsius case, as in other cases, is whether stakeholders would be better off with a quick liquidation of assets or a restructuring process that leaves intact any going concern value the company may have.[1] According to Celsius, a rushed liquidation of all assets (including their cryptocurrency assets) would result in far lower recoveries for creditors than if a new entity is set up to continue operating certain aspects of the businesses.

Prior to filing their Chapter 11 plan of reorganisation and disclosure statement, the Celsius debtors entered into an agreement with the Fahrenheit Group, under which Fahrenheit agreed to provide Celsius with operational expertise in exchange for an annual management fee of $35 million. Under this arrangement, Celsius creditors will still own 100% of the equity of the new crypto entity. Through the transactions contemplated in their Chapter 11 plan of reorganisation, creditors are slated to receive some form of the following three types of distributions: (a) liquid cryptocurrency (namely, BTC and/or ETH); (b) common stock in the new crypto entity; and (c) the proceeds from certain litigation brought against third parties, including former Celsius executives.

If the creditors do not approve the above-contemplated transaction, the Celsius debtors have proposed an alternative transaction structure, which they call the "Orderly Wind Down Plan". The Orderly Wind Down is to be conducted on the terms Celsius negotiated with the Blockchain Recovery Investment Consortium (BRIC), including Van Eck Absolute Return Advisers Corporation and GXD Labs LLC. The BRIC transaction anticipates providing recoveries to creditors in the following ways: (a) 100% of the equity interests in a publicly traded mining business with a potential management contract with GXD Labs LLC; (b) a

distribution of liquid cryptocurrency; and (c) a timely monetisation of the remaining Celsius assets and subsequent distributions of liquid cryptocurrency to creditors from the proceeds thereof.

On August 18, 2023, the Bankruptcy Court approved the Celsius debtors' disclosure statement, and the process of soliciting votes for the proposed Chapter 11 plan of reorganisation began soon thereafter. Pursuant to the Bankruptcy Court's order, creditors were given a little over one month to cast their ballot and/or object to confirmation of the plan of reorganisation. The plan of reorganisation being solicited contemplates 18 classes of creditors, nine of which are entitled to vote on the plan of reorganisation. Notably, general custody account holder claims, retail borrower claims, and Earn claims (discussed above) are entitled to vote on the plan of reorganisation.

Voyager

The problems faced by Voyager were a direct consequence of the failure of its "friends". 3AC, which defaulted on its loan repayment to Voyager and precipitated Voyager's bankruptcy filing, and FTX, whose declaration of bankruptcy shortly after committing to acquire Voyager's assets during the Chapter 11 restructuring process further exacerbated Voyager's situation, eventually culminating in its liquidation.

Voyager, founded in 2017 by Stephen Ehrlich, Philip Eytan, and Gaspard de Dreuzy, operated as a cryptocurrency brokerage. It allowed users to buy, sell, and trade cryptocurrencies, earning a reputation as one of the fastest-growing companies in the cryptocurrency sector. Listed in Canada, Voyager was one of the few publicly traded cryptocurrency companies. Voyager was notable for its user-friendly mobile app and innovative rewards programme, which incentivised customers to hold specific crypto assets, appealing to crypto enthusiasts seeking additional benefits.

The hazards of the interconnectedness of leverage and debt between crypto intermediaries became glaringly apparent in the rapid demise of several companies after the collapse of Terra Luna and the subsequent bankruptcy of 3AC. For Voyager, 3AC's bankruptcy proved fatal. When 3AC defaulted on its substantial loan of 15,250 Bitcoin and $350 million of USD Coin (USDC) to Voyager, it triggered Voyager's bankruptcy filing on July 5, 2023.

Voyager faced a series of unique challenges as the first of this recent group of crypto companies to navigate the U.S. bankruptcy process. An unusual complexity in the case was that the vast majority of creditors were individual account holders, and there was minimal secured debt. While there is a well-worn path for treating secured creditors in bankruptcy, a case where almost all of the indebtedness was to account holders who were unsecured creditors posed distinctive challenges. Like Genesis, Celsius, and FTX, account holders could not access their funds, which caused consternation among the account holder class. Consequently, we saw the emergence of social media platforms, notably X (f/k/a Twitter), where account holder creditors collaborated to share information and propose recovery optimisation strategies.

The Bankruptcy Court faced several issues of first impression to decide. As Josh Sussberg, Voyager's external bankruptcy counsel, remarked during a hearing, "I think for many of us this is unchartered territory". Valuing digital assets in bankruptcy was still a novel process, compounded by the volatile nature of cryptocurrencies. Prior to the Voyager filing (and subsequent Celsius, FTX, and Genesis filings), U.S. Bankruptcy Courts had never overseen cryptocurrency bankruptcy cases of this magnitude. Some of the most pressing questions facing the Court included the treatment of digital assets by the Court, the priority of creditors, whether customers would be paid back in crypto or fiat, and the treatment of cash held by Voyager's account holders held at Metropolitan Commercial Bank. Additionally, how would Voyager's own token be valued?

Another layer of complexity stemmed from the differing viewpoints of the company and its unsecured creditors regarding the ideal outcome of Voyager's bankruptcy. While Voyager sought to restructure the business as a going concern, there was a divergence among account holders on whether Voyager should reorganise or liquidate and return the remaining crypto assets to account holders.

On June 20, 2023, nearly a year after Voyager filed for Chapter 11 protection, creditors received their first distribution of cryptocurrency. The initial recovery of creditors amounted to approximately 35.72% of each account holder's crypto assets, though it varied based on individual crypto holdings. So, how did Voyager arrive at this point, and what lessons can be drawn from this experience? It became evident that crypto restructurings are exceptionally complex. Following an extensive auction process, Voyager could not find a buyer to continue its brokerage operations as a going concern. An agreement had initially been reached with FTX to sell certain assets, including all its cryptocurrency holdings, for $1.422 billion. The assets comprised $1.311 billion in cryptocurrency and an additional $111 million in value. However, this deal was cancelled on November 11, 2022, coinciding with FTX's own bankruptcy filing. Subsequently, Voyager entered into an asset sale with Binance.US on December 19, 2022, for $1.022 billion, encompassing $1.002 billion in cryptocurrency and $20 million in cash. Following months of negotiations and subsequent objections by U.S. regulatory authorities, Binance.US withdrew from the transaction on April 25, 2023. As a result, Voyager decided to proceed with liquidation, culminating in the first distribution to creditors on June 20, 2023.

FTX

FTX, a cryptocurrency exchange based in the Bahamas, quickly rose to prominence worldwide, particularly in the United States, through its associated entity, FTX.US. It represented the rapid growth and sudden dips experienced by many companies in the fast-paced crypto industry. Established in 2019, by 2021, FTX was the third-largest crypto exchange by volume.

The primary business of FTX centred around holding crypto assets and functioning as an exchange. Consequently, its consumers generally perceived no risk to their funds held by the company. Many esteemed venture investment funds, such as Sequoia Capital, purchased equity in FTX, further reassuring holders. Major investors were seen as backing the company, presumably after thorough due diligence. Additionally, FTX gained significant visibility as a high-profile political contributor and by acquiring the naming rights to the former American Airlines Arena in downtown Miami.

In September 2022, FTX successfully bid in a contested auction to acquire the assets of Voyager out of bankruptcy. Like many crypto-related businesses, FTX issued its own digital asset, the "FTT" token. The FTT token, which reached a peak market value of around $75.54, was sold to investors and the public. However, the token did not bestow any rights to profits at FTX or any real governing rights. It was somewhat akin to an airline affinity programme, but without a direct right to payment.

In 2022, FTX seemed to be expanding beyond crypto into gaming, venture capital, and even stock trading. To the public, FTX appeared to be the future – a resounding success with a valuation of over $32 billion. However, the reality was somewhat different.

From the outset, FTX was financially supported by a trading company called Alameda Research, co-founded by Sam Bankman-Fried, who later became the CEO and public face of FTX. Alameda dealt with crypto trading and helped maintain the market for FTT. Even though customer assets at FTX were supposed to be segregated, a large loan was made to Alameda using these assets as collateral, backed by FTT.

Due to either unsuccessful investments or a decline in the price of crypto, this loan could not be repaid. Consequently, FTX could not reimburse either its consumer creditors or larger crypto companies with which it had business ties. This resulted in the bankruptcy filings of BlockFi and Gemini Holdings. After a few weeks of frantic efforts by Sam Bankman-Fried to secure a lifeline, the company collapsed spectacularly, wiping out over $32 billion in shareholder value.

As media attention remains focused on Bankman-Fried's arrest and forfeiture of bail, the FTX bankruptcy case continues to move through the Delaware Bankruptcy Court system. Some assets have been sold, and various restructuring ideas have been proposed. While bankruptcy cases in the United States are typically costly, the FTX case appears to be exceptionally so. Professional fees are reported to be exceeding $1.5 million per day and are likely even higher.

BlockFi

BlockFi was founded in 2017 in Jersey City, New Jersey, by Zac Prince and Flori Marquez to provide credit services to markets with limited access to simple financial products. In subsequent years, the company's meteoric rise to financial prominence would cause its expansion into globally recognised financial and technological hubs like New York, Poland, Singapore, and Argentina. Unlike many of its competitors, BlockFi never launched its own token to raise funds, but instead relied on more traditional capital markets and venture funds. BlockFi was also the first company to seek and receive lending licences in multiple states to make cryptocurrency-backed loans, which ultimately helped the company reach its position as a leading provider of financial services in the cryptocurrency industry.

BlockFi's eventual bankruptcy was preceded by a series of significant industry events that strained its liquidity and left the company exposed to the collapse of one of its major lenders, FTX. BlockFi had significant exposure to FTX and its crypto trading partner, Alameda Research Ltd., through certain loan obligations and assets held on the FTX platform. Seeking to address its worsening liquidity shortfall, BlockFi entered into a $400 million loan facility with FTX in June of 2022. As part of the loan negotiations, FTX received an option to acquire BlockFi by requiring BlockFi Inc. to redeem and cancel all equity securities other than those issued to FTX. BlockFi's situation worsened when FTX's financial troubles became public in early November 2022 after leaked financials showed that FTX and Alameda had overstated their revenues and assets and faced regulatory scrutiny and litigation. FTX froze withdrawals on November 8, 2022, citing a "liquidity crunch". BlockFi froze withdrawals on November 10, 2022 to preserve its remaining assets and protect its clients. FTX filed for bankruptcy on November 11, 2022, with BlockFi filing shortly after on November 28, 2022.

As discussed above, BlockFi's bankruptcy was also preceded by the failures of other crypto lenders, Celsius and Voyager, which also halted withdrawals and filed for bankruptcy in June and July of 2022, respectively. The collapse of the renowned crypto hedge fund, 3AC, was another source of significant losses for BlockFi in relation to the fund's investment in Luna, a cryptocurrency issued by Terra, an open-source blockchain protocol that lost most of its value in May of 2022.

As of August 2023, the BlockFi bankruptcy case is nearing its conclusion, as the debtors have filed a joint Chapter 11 plan of reorganisation with the support of the Unsecured Creditors' Committee. According to the debtors, the current plan of reorganisation was formulated to provide for the return of digital assets and cash to clients on the fastest timeline possible. On August 2, 2023, the Bankruptcy Court conditionally approved the disclosure statement, which provides information about the plan of reorganisation and the

debtors' financial situation. The debtors are currently soliciting votes from creditors and other parties in interest on the plan of reorganisation. A hearing to approve the disclosure statement and confirm the plan of reorganisation is scheduled for September 26, 2023. The debtors have also requested an extension of their exclusive periods to file and solicit acceptance of the plan of reorganisation to allow time to complete the voting process, obtain final approval of the disclosure statement, confirm the plan of reorganisation, and allow the plan of reorganisation to become effective.

Exploring cryptocurrency-related cases: Challenges and insights

The crypto and blockchain-related cases mentioned earlier present unique and rarely encountered scenarios, posing distinct challenges to the bankruptcy process. These challenges stem from both the unconventional nature of the assets involved and the diverse makeup of the creditors. While each case has its nuances, common themes emerge, shedding light on the effectiveness of the U.S. Bankruptcy Code in handling these situations and areas where potential updates may be needed.

The empowered debtor in Chapter 11

When examining Chapter 11 bankruptcy cases in the United States, outsiders are often surprised by the substantial power wielded by the debtor, the company filing for bankruptcy. Chapter 11 essentially grants the debtor an order of protection to restructure its business without undue interference from creditors. With the twin goals of assisting a company in reorganising and providing creditors with a means to recover their debts, the Chapter 11 process heavily leans toward supporting debtors. Two potent examples of this debtor-friendly structure are (i) debtors are allowed to run their business as debtors-in-possession, in contrast to other systems where a trustee or liquidator runs the business, and (ii) the debtor is given the exclusive right to propose a plan of reorganisation or liquidation for a significant period (typically 120 days, although this period is often extended in complex Chapter 11 cases by motion of the debtors). The latter has the condition that if the debtor does not present a plan or fails to have it approved, the creditors or other parties in interest can propose their plan of reorganisation or liquidation.

However, concerns arise about the potential abuse of this power. Some debtors, driven by their interests and the fees of their professionals, might prolong a case when liquidation could have been a better option for creditors. In cases where assets are primarily in cryptocurrency, the depressed prices and the desire to wait for crypto values to rise before selling can exacerbate the situation. Additionally, debtors often seek releases for their executives under a plan of reorganisation, which can lead to choices favouring the debtor and its personnel over the interests of creditors. In certain scenarios, creditors find themselves in a precarious position when debtors prioritise third-party releases and exculpation for their executives, effectively pressuring creditors to accept less favourable terms to expedite the debtor's exit from bankruptcy.

Treatment of debtor-issued tokens

A compelling issue in these crypto cases revolves around how to treat "digital assets" issued by the debtor. Most of the debtors, besides BlockFi, issued proprietary digital tokens (e.g., FTT for FTX, CEL for Celsius, VGX for Voyager). These tokens did not represent equity or share in the company's profits, though the Securities and Exchange Commission (SEC) has, in some instances, challenged this classification. Despite these limitations, apart from Voyager, these tokens raised hundreds of millions of dollars through sales and boasted substantial market capitalisation on exchanges. In addition to the tokens sold to crypto purchasers, many were held by insiders or in the debtor's treasury.

Not easily identified as debt, equity, or affinity points, the status of these tokens remains unclear – are holders of a debtor's crypto considered creditors due to their holdings, contract counterparties, or something else entirely? While definitive answers are scarce, it seems that these tokens are not typically classified as debt. Complicating matters, depositors who participated in "Earn" or "Rewards" programmes (e.g., Celsius and Voyager) lost title to their assets in exchange for interest or rewards payments. Should these depositors be treated differently than holders of the debtor's token? The treatment varies case by case, with no subordination of the VGX token in Voyager and non-insider holders of CEL tokens also not being subordinated. Furthermore, the SEC's potential classification of digital assets as securities can complicate the distribution of crypto assets by the debtor back to creditors.

Who are the creditors, and who speaks for them?

The Bankruptcy Code establishes a process for an official committee of unsecured creditors (UCC) to collaborate with the debtor, the U.S. trustee, and the Court during the restructuring. The UCC comprises an assortment of creditors appointed by the U.S. trustee and is intended to represent the collective interest of creditors – rather than any specific creditor or type of creditor. The debtor's bankruptcy estate pays the UCC's professional fees before general creditors receive any distribution. In most of these crypto cases, the creditors consisted mainly of individuals, many with relatively small claims and who did not anticipate the risk to their funds. Many of these creditors believed that there was insurance on their deposited funds.

While the UCC sometimes reached agreements with debtors, hundreds of individual creditors filed objections – a substantially higher number than usual. The Courts took these objections seriously but rarely ruled in favour of creditors over debtors, given the complexity of the crypto industry and the judges' relative unfamiliarity with it. One accommodation provided by the Bankruptcy Code and Bankruptcy Courts is not requiring creditors who agreed with the listed amount and nature of their claim to file a proof of claim.

As these and other cases are worked through, it is worth considering whether the UCC effectively advocates for individual creditors, whether different types of creditor representation are needed, or whether the Bankruptcy Code should be revised to enhance consumer protection.

Conclusion

In summary, these cryptocurrency-related cases bring forth a myriad of intricate issues, including SEC scrutiny and the risks posed to consumers. It is worth acknowledging the commendable swiftness in which U.S. Bankruptcy Courts have handled these intricate proceedings. Nevertheless, lingering questions remain about the extremely high administrative costs, the debtor-centric nature of proposed reorganisations that, in some respects, favour debtors more, and the limited voice given to individual creditors.

Beyond the administrative intricacies, these bankruptcy cases are stark reminders of the perils of wishful thinking and the allure of opportunities that appear too good to be true. The interest rates offered by many of these Earn programmes would not withstand scrutiny of any form of serious diligence. The belief that "crypto is different" and is exempt from standard financial rules has proven misguided. While retail investors may not be expected to engage in exhaustive due diligence, numerous sophisticated investors overlooked obvious red flags.

A recurring theme throughout these cases is the excessive reliance on debt and exposure to problematic counterparties. Enhanced risk management, a culture of heightened caution, and comprehensive due diligence could have averted much of the ensuing pain and losses. In these cases, the immense potential of blockchain, decentralisation, and cryptocurrency was eclipsed by greed and inadequate risk management, missing the opportunities for these transformative technologies to thrive fully.

Endnote

1. In the Chapter 11 context, Section 1129(a)(7) of the Bankruptcy Code requires that a bankruptcy court determine that a Chapter 11 plan provides, with respect to each class, that each holder of a claim or an equity interest in such class either (i) has accepted the plan, or (ii) will receive under the plan value that is not less than the amount that such holder would receive if the debtors had liquidated under Chapter 7 of the Bankruptcy Code. Therefore, creditors who vote to reject a Chapter 11 plan may have grounds to object to confirmation of the plan if they would stand to receive a larger recovery for their claim through a liquidation process under Chapter 7.

Stephen Rutenberg
Tel: +1 917 623 8121 / Email: srutenberg@polsinelli.com

Stephen Rutenberg specialises in the intersection of special situations investing and FinTech, with a particular focus on cryptocurrency and blockchain technology, co-heading the firm's FinTech and blockchain practice to provide market-leading perspectives on the innovative utilisation of blockchain, digital assets, and Web3 technology. Stephen counsels clients on a broad array of special situations-related matters, including transactions involving the purchase of distressed assets, such as loans and bankruptcy claims, workouts, capital raising, and other liquidity transactions.

Stephen is admitted to practise law in New York and Florida and is also a solicitor in England and Wales. Currently living in Florida, Stephen is a former board member of the UJA-Federation of New York and received the James H. Fogelson Emerging Leadership Award from the UJA-Federation of New York in February 2017 for his contributions to the legal and philanthropic communities in New York.

David Brill
Email: davidhbrill@gmail.com

David Brill is a seasoned technology and financial services executive with a rich history in the digital asset space long before the term "FinTech" gained widespread recognition. He is a true pioneer in the digital asset industry, having played pivotal roles in several of its early milestones. Notable achievements include facilitating the listing of Ethereum on one of the first regulated digital asset exchanges, contributing to the development of the initial Exchange-Traded Fund (ETF) filing with the Securities and Exchange Commission, and offering strategic consulting expertise to numerous high-profile digital asset projects.

Mr. Brill is a management consultant and the Chair of the Cryptoassets Working Group within the WSBA, where he focuses on digital asset trading and investing. His illustrious career encompasses a series of influential positions, including as the Former Deputy General Counsel of Voyager Digital, General Counsel of OST, General Counsel of Gemini Trust Company, and Executive Vice President and General Counsel of American Stock Transfer & Trust Company, and as a senior lawyer for Thomson Reuters.

Michael DiPietro
Tel: +1 302 252 0939 / Email: mdipietro@polsinelli.com

Michael DiPietro advises clients on corporate restructuring, bankruptcy litigation, distressed asset sales, and other insolvency matters. Michael represents debtors, lenders, and other parties in interest in a variety of Chapter 11 cases. A significant component of Michael's practice relates to his work on the intersection of insolvency and FinTech, including cryptocurrency and blockchain technology. He works closely with Polsinelli attorneys to help protect clients' interests and counsels both debtors and creditors.

During his time at Temple University's Beasley School of Law, Michael served as a legal extern to the Honorable Richard A. Lloret, U.S. District Court for the Eastern District of Pennsylvania.

Polsinelli

315 Biscayne Boulevard Suite 400, Miami, FL 33131, USA
Tel: +1 305 921 1800 / URL: www.polsinelli.com

Australia

Peter Reeves, Robert O'Grady & Emily Shen
Gilbert + Tobin

Government attitude and definition

Australia is historically a neutral and stable jurisdiction for blockchain and cryptocurrency businesses. This has enabled significant growth driven, in part, by the Commonwealth Government of Australia's (**Government**) supportive approach for new and innovative financial services and products in the financial technology (**fintech**) sector. While growth remains, the pace has moderated in recent years. This is due to headwinds from lower global economic growth, turbulent crypto business closures, increased regulatory enforcement and the Government's relative inaction in pushing forward crypto policy and legislation.

Clarity regarding the application of Australian regulatory regimes to the blockchain and cryptocurrency sector has been iterative. Digital currencies have been captured under the anti-money laundering and counter-terrorism financing (**AML/CTF**) regime since 2018, reflective of growing recognition towards digital currencies as a method of transferring value and the associated money laundering and terrorism financing (**ML/TF**) risks. In 2021, Australia's primary corporate, markets, consumer credit and financial services regulator, the Australian Securities and Investments Commission (**ASIC**), clarified its expectations for crypto assets that form part of the underlying assets of exchange-traded products (**ETPs**) and other investment products (set out in *ASIC Information Sheet 230* (**INFO 230**)). This is in addition to ASIC's expectations regarding the regulatory status of certain crypto assets (set out in *ASIC Information Sheet 225* (**INFO 225**)).

2022 saw a raft of government reviews into both the cryptocurrency and fintech sectors, recommending expanded and clarified regulatory regimes for cryptocurrencies and payments. In 2022, Australian Treasury (**Treasury**) consulted on a proposed regulatory framework for crypto asset secondary service providers (**CASSPrs**). The proposals broadly reflected the regime for financial services providers, with scope for tailored application to address the nuances of crypto asset services. The CASSPr consultation coincided with a change of Government and the proposals were suspended in favour of a token mapping consultation. Treasury commenced this consultation in early 2023 to define digital asset types and identify gaps in the current regulatory framework. While the consultation did not include any demonstrative proposals for new regulation, it was a key step in the Government's plans to regulate the crypto sector. The Government indicated an intention to release a licensing and custody paper for crypto asset service providers in mid-2023. However, at the time of writing, this has not yet been released and it is unclear whether this will draw on the previous CASSPr consultation.

On 29 March 2023, opposition Senator Andrew Bragg introduced a private member's bill, *Digital Assets (Market Regulation) Bill 2023* (**Digital Assets Bill**), which proposes to regulate digital assets, including by introducing licensing requirements for digital asset exchanges, digital asset custody service providers and stablecoin issuers. The Digital

Assets Bill also proposes to introduce disclosure requirements for facilitators of central bank digital currencies (**CBDCs**) in Australia. The proposed licensing framework leans on familiar concepts and requirements under the financial services licensing regime. While the Digital Assets Bill represents a tangible attempt at crypto legislation, the Bill was not introduced by the current Government and is a private member's bill introduced by Senator Bragg. At the time of writing, the Digital Assets Bill remains before parliament.

This backdrop of uncertainty has been underpinned by regulators (primarily ASIC) pursuing high-profile enforcement actions against crypto businesses. These actions have focused on alleged unlicensed activities and the nature of associated conduct (e.g., perceived instances of investor and consumer risks with crypto-adjacent businesses). While this reflects ASIC's 2022–26 Corporate Plan and 2023 Enforcement Priorities focusing on consumer protection, the "regulate by enforcement" approach adopted to date has strengthened calls for legislative clarity.

The Reserve Bank of Australia (**RBA**), Australia's central bank, indicates no immediate plans to issue a retail CBDC. However, it indicates a perceived use for wholesale CBDCs and is currently undertaking various industry research projects to explore use cases and economic benefits of a CBDC in Australia. This coincides with a Treasury consultation that proposes to provide the RBA with expanded scope to regulate stablecoin payment systems that become fundamental to Australia's payments infrastructure. At the time of writing, this consultation remains on foot and it is expected that regulatory supervision of stablecoin systems will be implemented in coming years.

Cryptocurrency regulation

While there have been legislative amendments to accommodate the use of cryptocurrencies, to date these have predominantly focused on the transactional relationships (e.g., the issuing and exchanging process) and activities involving cryptocurrencies, rather than the cryptocurrencies themselves. As set out above, Treasury has undertaken (and continues to undertake) multiple consultations to clarify the nature of digital assets and how the associated risks translate to a regulatory framework for crypto asset service providers. These consultations are maintaining the focus of managing risks through regulating centralised entities rather than individual assets or decentralised (or distributed) structures.

In the context of its recent enforcement actions, ASIC reaffirms the view that legislative obligations and regulatory requirements are technology-neutral and apply irrespective of the mode of technology that is being used to provide a regulated service. While there is currently no legislation created to deal with cryptocurrencies as a discrete area of law, this does not prevent them from being captured within existing regimes under Australian law (see under "Sales regulation" below).

ASIC's regulatory guidance informs businesses of its approach to the legal status of crypto assets. This turns on how they are structured and the rights attached, which ultimately determines the regulations with which an entity must comply. For example:

- Cryptocurrency that is, or forms part of a collective investment product that is, a financial product under the *Corporations Act 2001* (Cth) (**Corporations Act**) will fall within the scope of Australia's existing financial services regulatory regime. See "Sales regulation" for further information.
- There has also been a proliferation of cryptocurrency lending activities. Where such activities fall within the scope of the credit activities and services caught under the *National Credit Consumer Protection Act 2009* (Cth) (**NCCP Act**), the relevant entities may need to hold an Australian credit licence or be otherwise exempt from this requirement.

ASIC has clarified expectations for crypto assets that form part of the underlying assets of ETPs and other investment products (see INFO 230). In INFO 230, ASIC sets out expectations for market operators, retail fund operators (i.e., responsible entities), listed investment entities (including listed investment trusts and listed investment companies) and Australian financial services licence (**AFSL**) holders dealing in crypto assets. This primarily centres around criteria that ASIC expects market operators to apply when determining whether a specific crypto asset is an appropriate asset for market-traded products. This broadly requires institutional support of the crypto asset, service providers willing to support ETPs that invest in or provide exposure to the crypto asset, maturity of the spot market for the crypto asset, regulation of derivatives linked to the crypto asset, and the availability of robust and transparent pricing mechanisms for the crypto asset. ASIC has commented that (as at October 2021) it considers Bitcoin and Ether likely satisfy ASIC's criteria for determining appropriate underlying assets for an ETP. ASIC has also included good practices in relation to how fund asset holders are required to custody crypto assets, as well as ensuring that adequate risk management systems are in place. While ASIC has provided this clarity, recent enforcement actions indicate that it considers crypto assets to be an appropriate investment asset for retail clients in very limited circumstances.

There are currently no specific regulations dealing with blockchain or other distributed ledger technology (**DLT**) in Australia. However, ASIC maintains a public information sheet (*INFO 219 Evaluating distributed ledger technology*) outlining its approach to the regulatory issues that may arise through the implementation of blockchain technology and DLT solutions more generally. Businesses considering operating market infrastructure, or providing financial or consumer credit services using DLT, will remain subject to the compliance requirements that currently exist under the applicable licensing regime. There is a general obligation that entities relying on technology in connection with the provision of a regulated service must have the necessary organisational competence and adequate technological resources and risk management plans in place. While the existing regulatory framework is sufficient to accommodate current implementations of DLT, as the technology matures, additional regulatory considerations will arise.

Various cryptocurrency networks have also implemented "smart" or self-executing contracts. These are permitted in Australia under the *Electronic Transactions Act 1999* (Cth) (**ETA**) and the equivalent Australian state and territory legislation. The ETA provides a legal framework to enable electronic commerce to operate in the same way as paper-based transactions. Under the ETA, self-executing contracts are permitted in Australia, provided they meet all the traditional elements of a legal contract.

Sales regulation

The sale of cryptocurrency and other digital assets is regulated by Australia's existing financial services regulatory regime. Core considerations for issuers are outlined below.

Licensing

Entities carrying on a financial services business in Australia must hold an AFSL or be exempt. Therefore, persons providing financial services in relation to crypto assets that constitute financial products will trigger the AFSL requirement and associated compliance and disclosure requirements. The definitions of "financial product" and "financial service" under the Corporations Act are broad and ASIC has indicated in INFO 225 that crypto assets with similar features to existing financial products will trigger the relevant regulatory obligations.

As above, ASIC indicates (in INFO 225) that the legal status of crypto assets turns on their structure and the associated rights (which ASIC interprets broadly). Depending on the circumstances, crypto assets may constitute interests in managed investment schemes (collective investment vehicles), securities, derivatives, or fall into a category of more generally defined financial products, all of which are subject to AFSL regulation. In INFO 225, ASIC provides high-level regulatory signposts for crypto asset participants to determine whether they have legal and regulatory obligations. These signposts are relevant to crypto asset issuers, crypto asset intermediaries, miners and transaction processors, crypto asset exchanges and trading platforms, crypto asset payment and merchant service providers, wallet providers and custody service providers, and consumers.

Entities dealing in financial product crypto assets will need to comply with the regulatory requirements under the Corporations Act, which generally include disclosure, registration, licensing and conduct obligations. An entity that facilitates payments by crypto assets may also be required to hold an AFSL and the operator of a crypto asset exchange may be required to hold an Australian market licence if the supported assets are financial products.

As noted, Treasury continues to consult on a proposed licensing regime for crypto asset service providers. While the form of any proposals remains unknown, it is expected that any regime will focus on service providers that deal in crypto assets generally (that is, financial product and non-financial product crypto assets), as well as tailored inclusions for financial services providers dealings in financial product crypto assets. See "Government attitude and definition" for further information.

Concurrently, the Australian Law Reform Commission (**ALRC**) is conducting an inquiry into simplifying Australia's overarching financial services regulatory framework to make it "more adaptive, efficient and navigable for consumers and regulated entities". As part of the inquiry, the ALRC has provided interim reports on three areas, being the design and use of definitions in corporations and financial services legislation, the regulatory design and hierarchy of laws, and the potential to reframe or restructure financial services laws. A consolidated report is due on 30 November 2023; however, it remains to be seen whether any proposals will address crypto as an asset class.

Marketing

As crypto asset sales may involve an offer of financial products, this has marketing implications. For example, financial product offers to retail clients (with some exceptions) must be accompanied by a regulated disclosure document (e.g., a product disclosure statement or a prospectus and a financial services guide) that satisfies the content requirements of the Corporations Act and regulatory guidance published by ASIC. Such a disclosure document must set out prescribed information, including benefits and risks of the product, as well as the provider's fee structure, to assist a client in deciding whether to acquire the crypto asset from the provider. In some instances, the marketing activity itself may cause the sale to be an offer of a regulated financial product.

Depending on the investor's status as a wholesale client, an offer of financial products may not require regulated disclosure under the Corporations Act.

Cross-border issues

Carrying on a financial services business in Australia will require a foreign financial services provider (**FFSP**) to hold an AFSL, unless an exemption applies. Notably, the Corporations Act may apply to crypto asset sales regardless of whether they are created and offered from Australia or overseas. At the time of writing, Australia's treatment of

regulated offshore entities is in a state of flux. Historically, FFSPs regulated in comparable jurisdictions had the benefit of limited licensing relief for financial services provided to wholesale clients. In 2020, this was repealed and replaced with a foreign AFSL regime. In 2021, the Government proposed reverting back to the comparable jurisdiction regime (with some amendments). This proposal was put to Australian parliament in early 2022; however, the proposed legislation lapsed with the change of Government. At the time of writing, there has been no intention announced regarding the future of FFSP regulation in Australia. An announcement is expected in late 2023, and it is broadly expected that a form of comparable jurisdiction relief will be reintroduced.

Foreign companies taken to be carrying on a business in Australia, including by dealing in crypto assets, may be required to either establish a local presence (i.e., register with ASIC and create a branch) or incorporate a subsidiary. Broadly, the greater the level of system, repetition or continuity associated with an entity's business activities in Australia, the greater the likelihood that registration will be required. Generally, a company holding an AFSL will be carrying on a business in Australia and will trigger the requirement.

Marketing financial product crypto assets to Australian residents from offshore may still trigger licensing and disclosure requirements. Generally, an offshore service provider may respond to requests for information and issue products to an Australian resident if the resident makes the first (unsolicited) approach and there has been no conduct on the part of the issuer designed to induce the investor to make contact, or activities that could be misconstrued as the provider inducing the investor to make contact.

Design and distribution obligations and product intervention powers

Since October 2021, issuers and distributors of financial products must comply with design and distribution obligations (**DDO**), which may impact the way crypto assets are structured and sales are conducted. Issuers and distributors must implement effective product governance arrangements, which include (among other things) creating and distributing target market determinations (**TMDs**) in relation to retail clients acquiring the relevant financial products. The DDO aims to ensure that financial products are targeted at the correct category of potential customers, and disclosures regarding the adequacy and suitability of the product for the target market are required to be accurate and timely.

ASIC also has product intervention powers where there is a risk of significant consumer detriment, enabling ASIC to address market-wide problems or specific business models and deal with certain "first mover" issues. The power covers financial products under the Corporations Act and *Australian Securities and Investments Commission Act 2001* (Cth) (**ASIC Act**) and credit products under the NCCP Act.

In ASIC's 2022–26 Corporate Plan, ASIC has identified product design and distribution as one of its key strategic priorities, and has been actively enforcing this space. ASIC issued its first DDO stop orders in July 2022 in response to deficiencies in TMDs made under the DDO regime. Between July 2022 and June 2023, ASIC issued 41 stop orders to prevent consumers and investors being targeted by products that may be inappropriate for their objectives, financial situation and needs. This included three stop orders preventing the distribution of crypto funds associated with alleged deficient TMDs. ASIC's powers are likely to impact marketing and distribution practices in the crypto asset sector where they fall within its remit.

Consumer law

Even if a crypto asset sale is not regulated under the Corporations Act, it may remain subject to other regulation and laws, including the Australian Consumer Law set out at Schedule 2 to the *Competition and Consumer Act 2010* (Cth) (**ACL**) relating to the offer of services or

products to Australian consumers. The ACL prohibits misleading or deceptive conduct in a range of circumstances, including in the context of marketing and advertising. Therefore, care must be taken in crypto sale promotional material to ensure that it does not contain false information and that buyers are not misled or deceived. Additionally, promoters and sellers are prohibited from engaging in unconscionable conduct and must ensure that the issued crypto assets are fit for their intended purpose. The protections of the ACL are generally reflected in the ASIC Act, providing substantially similar protection to investors in financial products or services.

ASIC has also received delegated powers from the Australian Competition and Consumer Commission to enable it to take action against misleading or deceptive conduct in marketing or issuing crypto asset sales (regardless of whether it involves a financial product). ASIC has indicated that misleading or deceptive conduct in relation to crypto asset sales may include:

- using social media to create the appearance of greater levels of public interest;
- creating the appearance of greater levels of buying and selling activity for a crypto asset by engaging in (or arranging for others to engage in) certain trading strategies;
- failing to disclose appropriate information about the sale; or
- suggesting that the sale is a regulated product or endorsed by a regulator when it is not.

ASIC has stated that it will use this power to issue further inquiries into crypto asset issuers and their advisers to identify potentially unlicensed and misleading conduct.

A range of consequences may apply for failing to comply with the ACL or the ASIC Act, including monetary penalties, injunctions, compensatory damages and costs orders.

Taxation

The taxation of cryptocurrency in Australia has been an area of much debate, despite recent attempts by the Australian Taxation Office (**ATO**) to clarify the operation of the tax law. For income tax purposes, the ATO views cryptocurrency as an asset that is held or traded (rather than as money or a foreign currency). On 23 June 2023, *Treasury Laws Amendment (2022 Measures No. 4) Bill 2022* received royal assent, which clarifies that cryptocurrencies are not foreign currencies for income tax purposes.

The tax implications for holders of cryptocurrency depend on the purpose for which the cryptocurrency is acquired or held. The summary below applies to holders who are Australian residents for tax purposes.

Sale or exchange of cryptocurrency in the ordinary course of business

If a holder of cryptocurrency is carrying on a business that involves sale or exchange of the cryptocurrency in the ordinary course of that business, the cryptocurrency will be held as trading stock. Gains on the sale of the cryptocurrency will be assessable and losses will be deductible (subject to integrity measures and "non-commercial loss" rules). Examples of relevant businesses include cryptocurrency trading and cryptocurrency mining businesses.

Whether or not a taxpayer's activities amount to carrying on a business is a question of fact and degree, and is ultimately determined by weighing up the taxpayer's individual facts and circumstances. Generally (but not exclusively), where the activities are undertaken for a profit-making purpose, are repetitious, involve ongoing effort, and include business documentation, the activities would amount to the carrying on of a business.

Isolated transactions

Even if a holder of cryptocurrency did not invest or acquire the cryptocurrency in the ordinary course of carrying on a business, profits or gains from an "isolated transaction"

involving the sale or disposal of cryptocurrency may still be assessable where the transaction was entered into with a purpose or intention of making a profit, and the transaction was part of a business operation or commercial transaction.

Cryptocurrency investments

If cryptocurrency is not acquired or held in the course of carrying on a business, or as part of an isolated transaction with a profit-making intention, a profit on sale or disposal should be treated as a capital gain. In this regard, the ATO has indicated that cryptocurrency is a capital gains tax (**CGT**) asset. Capital gains may be discounted under the CGT discount provisions, so long as the taxpayer satisfies the conditions for the discount (for example, the cryptocurrency is held for at least 12 months before it is disposed of).

Although cryptocurrency may be a CGT asset, a capital gain arising on its disposal may be disregarded if the cryptocurrency is a "personal use asset" and it was acquired for A$10,000 or less. Capital losses made on cryptocurrencies that are personal use assets are also disregarded. Cryptocurrency will be a personal use asset if it was acquired and used within a short period of time for personal use or consumption (that is, to buy goods or services).

Note that the ATO's view on the income tax implications of transactions involving cryptocurrencies is in a state of flux due to the rapid evolution of both cryptocurrency technology and its uses. On 21 March 2022, the Government released the Terms of Reference for a review to be undertaken by the Board of Taxation into the appropriate policy framework for the taxation of digital assets and transactions in Australia. In August 2022, the Board of Taxation published a consultation guide. In this respect, the Board of Taxation has been asked to report back to the Government by 30 September 2023.

Staking cryptocurrency

An entity may hold units of cryptocurrency (i.e., tokens) to validate and verify transactions within a blockchain. The "validator" may be rewarded with additional tokens for its role in this process. Token holders who participate in proxy staking or who vote their tokens in "proof of stake" or other consensus mechanisms may also be rewarded with additional tokens. The value of such tokens should be treated as ordinary income of the recipient at the time they are derived.

Issuers of cryptocurrencies

In the context of an initial coin offering (**ICO**), a coin issuance by an entity that is either an Australian tax resident, or acting through an Australian "permanent establishment", may be assessable in Australia. The current corporate tax rate in Australia is either 25% or 30%, depending on whether the issuer is considered a "base rate entity".

Australian goods and services tax (**GST**)

Supplies and acquisitions of digital currency made from 1 July 2017 are not subject to GST on the basis that they will be input-taxed financial supplies. Consequently, suppliers of digital currency will not be required to charge GST on these supplies, and a purchaser would *prima facie* not be entitled to GST refunds (i.e., input tax credits) for these corresponding acquisitions. On the basis that digital currency is a method of payment, as an alternative to money, the normal GST rules apply to the payment or receipt of digital currency for goods and services.

The term "digital currency" in the GST legislation requires that it is a digital unit of value that has all the following characteristics:

- it is fungible and can be provided as payment for any type of purchase;
- it is generally available to the public free of any substantial restrictions;

- it is not denominated in any country's currency issued by, or under the authority of, the relevant government agency;
- the value is not derived from or dependent on anything else; and
- it does not give an entitlement or privileges to receive something else.

In relation to a holder carrying on an enterprise of cryptocurrency mining, whether or not GST is payable by the miner on its supply of new cryptocurrency depends on a number of factors, including its specific features, whether the miner is registered for GST, and whether the supply is made in the course or furtherance of the miner's enterprise.

A miner will carry on an enterprise where it conducts an activity, or a series of activities, in the form of business or in the form of an adventure or concern in the nature of trade, but it does not include activities conducted for a private recreational pursuit, as a hobby or as an employee. The scope of carrying on an "enterprise" can be broader than carrying on a "business" (as outlined above), and some miners may unintentionally be carrying on an "enterprise" for GST purposes.

The specific features of cryptocurrency include it: being a type of security or other derivative; being "digital currency" as defined in the GST legislation; or providing a right or entitlement to goods or services. If the cryptocurrency is a security, derivative or "digital currency", its supply will not be subject to any GST because it will be an input-taxed financial supply (assuming the other requirements are satisfied).

A cryptocurrency miner would generally be required to register for GST if its annual GST turnover is A$75,000 or more, excluding the value of its supplies of digital currencies and other input-taxed supplies. However, a miner who does not satisfy this GST registration threshold may nevertheless elect to register for GST in order to claim from the ATO full input tax credits (i.e., GST refunds) for the GST cost of its business acquisitions (but acquisitions that relate to the sales or acquisitions of securities, derivatives or digital currencies are *prima facie* non-creditable or non-refundable).

A supply made in connection with a miner's enterprise, including the enterprise's commencement or termination, will generally be "made in the course or furtherance" of their enterprise, and may attract GST should other requirements be satisfied.

Enforcement

The ATO has created a specialist task force to tackle cryptocurrency tax evasion. The ATO also collects bulk records from Australian cryptocurrency designated service providers to conduct data matching to ensure that cryptocurrency users are paying the right amount of tax. With the broader regulatory trend around the globe moving from guidance to enforcement, it is likely that the ATO will also continue to tighten its scrutiny of cryptocurrency.

Money transmission laws and anti-money laundering requirements

Digital currency exchange (**DCE**) providers are required to register and enrol with the Australian Transaction Reports and Analysis Centre (**AUSTRAC**) as a reporting entity under Australia's AML/CTF regulatory framework. There is a penalty of up to two years' imprisonment or a fine of up to A$137,500, or both, for failing to register. Broadly, registered exchanges will be required to implement know-your-customer processes to adequately verify the identity of their customers, with ongoing reporting obligations such as annual compliance reporting and the requirement to monitor and report suspicious and large transactions. Exchange operators must also keep certain records relating to customer identification and transactions for up to seven years. DCE providers are required to renew their registration every three years.

The DCE sector has been of great interest to AUSTRAC, in particular monitoring the ML/TF risks associated with digital currency. In April 2022, AUSTRAC released a financial crime guide to preventing the criminal abuse of digital currencies. In April 2023, the Attorney General's Department announced its consultation on long-awaited reform to Australia's AML/CTF regime. Among the matters are proposed changes to:

- how digital currency exchanges are regulated from an AML/CTF perspective. The consultation proposes expanding the types of regulated services to cover exchanges between one or more other forms of digital currency, transfers of digital currency on behalf of a customer, safekeeping or administration of digital currency and provision of financial services related to an issuer's offer and/or sale of a digital currency; and
- update the travel rule and extend its application to remitters and digital currency exchange providers. The consultation proposes to update the travel rule to align with international standards by requiring payer and payee information for transfers on behalf of customers to other businesses, payer information to be verified and the inclusion of payee information.

The Attorney General's Department intends to consult further throughout 2023.

Promotion and testing

Subject to recent events, regulators in Australia have generally been receptive to new technology (including blockchain and cryptocurrency) and have sought to improve their understanding of, and engagement with, businesses by regularly consulting with industry on proposed regulatory changes. Both ASIC and AUSTRAC have established Innovation Hubs designed to assist new market entrants (including those operating in the blockchain and cryptocurrency sectors) more broadly in understanding their obligations under Australian law. ASIC has also entered into a number of cooperation agreements with overseas regulators, which aim to further understand the regulatory approach and product offerings in other jurisdictions (as discussed below).

ASIC Innovation Hub

The ASIC Innovation Hub is designed to foster innovation that could benefit consumers by helping Australian start-ups (including those operating in the blockchain and cryptocurrency sectors) navigate the Australian regulatory system. The Innovation Hub provides tailored information and access to informal assistance intended to streamline the AFSL process for innovative fintech start-ups, which could include cryptocurrency-related businesses.

In 2016, ASIC established the fintech regulatory sandbox, which included a fintech licensing exemption to allow businesses to test certain financial services, financial products and credit activities without holding an AFSL or Australian credit licence. This had strict eligibility requirements for both the type of businesses and the products and services that qualify for the licensing exemption, as well as restrictions on how many persons can be serviced and caps on the value of the financial products or services that can be provided. In 2020, the Government passed regulation to enhance this regulatory sandbox (aptly named the "enhanced regulatory sandbox"), which expanded the scope of the sandbox to test a broader range of financial services and credit activities for up to 24 months. This is broadly considered to better support innovation in the sector by increasing the cap restrictions as well as providing more nuanced parameters for clients that can be serviced.

Cross-border business

ASIC engages with regulators overseas to deepen its understanding of innovation in financial services, including in relation to cryptocurrencies. In particular, ASIC's enhanced cooperation agreement with the United Kingdom's Financial Conduct Authority remains

on foot, which allows the two regulators to, among other things, information-share, refer innovative businesses to each regulator's respective regulatory sandbox, and conduct joint policy work. ASIC also currently has either information-sharing or cooperation agreements with regulators in jurisdictions such as Austria, Brazil, Canada, China, Germany, Hong Kong, Indonesia, Israel, Italy, Japan, Kenya, Luxembourg, New Zealand, Singapore, Switzerland and the United States of America. These arrangements facilitate the cross-sharing of information on a range of market trends, many encouraging referrals of new market entrants (including those in the blockchain and cryptocurrency sector), and share insights from proofs of concepts and innovation competitions.

ASIC is also a signatory to the IOSCO Multilateral Memorandum of Understanding, which has committed over 100 regulators to mutually assist and cooperate with each other, particularly in relation to the enforcement of securities laws.

ASIC has committed to supporting financial innovation in the interests of consumers by joining the Global Financial Innovation Network, which is an international network of financial regulators and related organisations dedicated to facilitating regulatory collaboration in a cross-border context and providing more efficient means for innovative businesses to interact with regulators.

AUSTRAC Innovation Hub

AUSTRAC's Fintel Alliance is a private-public partnership seeking to adopt innovative approaches to combatting financial crime, including by adopting new technology and ways of working with government and industry. This includes setting up an Innovation Hub targeted at designing and testing technology solutions (including assessing the impact of emerging technology like blockchain and cryptocurrency), and setting up an Operations Hub to facilitate the exchange of financial intelligence for analysis. In its 2021–22 Annual Report, the Fintel Alliance noted a key working group from the alliance focused on tax evasion using virtual assets.

Ownership and licensing requirements

At the time of writing, there are no explicit restrictions on investment managers owning cryptocurrencies for investment purposes. However, investment managers may be subject to the AFSL regime where the cryptocurrencies held are deemed to be "financial products" and the investment managers' activities in relation to those cryptocurrencies are deemed to be the provision of financial services.

For example, investment managers providing investment advice on financial product cryptocurrencies will be providing financial product advice and must hold an AFSL or otherwise be exempt from this requirement. ASIC has provided significant guidance in relation to complying with the relevant advice, conduct and disclosure obligations, as well as the conflicted remuneration provisions under the Corporations Act. Further, investment managers may be required to hold an AFSL with a custodial or depository authorisation or be exempt from this requirement if they wish to custody financial product cryptocurrencies on behalf of clients. In relation to cryptocurrencies that form the underlying assets of ETPs, investment managers will need to consider ASIC's expectations in INFO 230 regarding the appropriateness of such assets within the overall profile of the ETP (see "Cryptocurrency regulation" for further information).

Australia has also seen expansion in robo-advice or digital advice models (including algorithmic or automated financial product advice without a human advisor). For investment or fund businesses seeking to operate in Australia by providing digital or hybrid advice

(including with respect to investing in cryptocurrencies), there are licensing requirements under the Corporations Act. ASIC guidance contained in *Regulatory Guide 255: Providing digital financial product advice to retail clients* details issues that digital advice providers need to consider generally, during the AFSL application stage and when providing digital financial product advice to retail clients, and complements ASIC's existing guidance on providing financial product advice, including *Regulatory Guide 36: Licensing: Financial product advice and dealing*. It is expected that there will be additional change in the financial advice sector (including the provision of digital advice) following the release of the Quality of Advice Final Report and the Government's consultation on its Delivering Better Financial Outcomes package, which adopts key recommendations from the final report. The Government expects to issue its final response later in 2023.

Financial product advisers also need to consider their conduct and disclosure obligations. ASIC has released *Regulatory Guide 175: Licensing: Financial product adviser – conduct and disclosure* with respect to this.

Mining

At the time of writing, there are no prohibitions on mining Bitcoin or other cryptocurrencies in Australia.

Cryptocurrency mining taxation

As above, the taxation of cryptocurrency and associated activities in Australia has been an area of much debate, and this has extended to taxation relating to mining cryptocurrency. See "Taxation" above for further information.

Cybersecurity

With the rise of cloud-based Bitcoin mining enterprises in Australia, mining businesses should carefully consider cybersecurity issues in relation to mining activities.

In its 2022–26 Corporate Plan, ASIC stated that a key priority is for ASIC to work with industry and other regulators to enhance cyber resilience, particularly given that the COVID-19 pandemic has accelerated technological trends. ASIC notes that there has been an increasing number of high-profile cyber attacks, and this has resulted in growing awareness in the industry of the importance of cyber resilience and enhanced investment in digital infrastructure to prevent data breaches, technology failures and system outages.

ASIC has also released regulatory guidance to help firms improve their cyber resilience, including reports, articles and practice guides. ASIC's most recent report, *Report 716 Cyber resilience of firms in Australia's financial markets: 2020–21*, identifies key trends in cyber resilience practices and highlights existing good practices and areas for improvement. The report builds on ASIC's last look into the cyber resilience of firms in Australia's financial markets, being *Report 651 Cyber resilience of firms in Australia's financial markets: 2018–19* and notes that there has been a small but steady improvement in cyber resilience, but that such improvement has not met the anticipated targets as a result of factors such as the pandemic, escalated threats and overly ambitious targets. ASIC has also previously provided two other reports, *Report 429 Cyber resilience: Health check* and *Report 555 Cyber resilience of firms in Australia's financial markets*, which examine and provide examples of good practices identified across the financial services industry. The reports contain questions that board members and senior management of financial organisations should ask when considering cyber resilience.

In June 2023, ASIC invited regulated entities to anonymously take part in a survey to measure cyber resilience in Australia's corporate and financial markets. The survey has been designated to assist entities with assessing its ability to govern and manage cyber risks, identify and protect critical information assets and detect, respond to and recover from cybersecurity incidents. ASIC intends to publish a report with key findings. Participants can elect to receive an individual report containing comparative insights.

Border restrictions and declaration

There are currently no border restrictions or obligations to declare cryptocurrency holdings when entering or leaving Australia.

The *Anti-Money Laundering and Counter-Terrorism Financing Act 2006* (Cth) (**AML/CTF Act**) mandates that both individuals and businesses must submit reports where physical currency in excess of A$10,000 (or foreign currency equivalent) is brought into or taken out of Australia. This requirement is restricted to "physical currency", which AUSTRAC has defined as being any coin or printed note of Australia or a foreign country that is designated as legal tender, and is circulated, customarily used and accepted as a medium of exchange in the country of issue. Although market commentary indicates that some governments have created or are attempting to issue official cryptocurrencies, the intangible nature of cryptocurrency remains a bar to it being captured by declaration obligations under the AML/CTF Act.

While the AML/CTF Act was amended to address some aspects of cryptocurrency transfer and exchange in 2017, this amendment did not see the scope of AML/CTF regulation widen the border restrictions. At the time of writing, there appears to be no indication that any such further amendment to include border restrictions is being contemplated, but there is ongoing consultation on expanding the application of the AML/CTF regime to digital currency exchanges. See "Money transmission laws and anti-money laundering requirements" for further details.

Reporting requirements

The AML/CTF Act imposes obligations on entities that provide certain "designated services" with an Australian connection. Generally, the AML/CTF Act applies to any entity that engages in financial services or credit (consumer or business) activities in Australia, including the provision of DCE services. These obligations include record-keeping and reporting requirements.

For example, AML/CTF legislation outlines reportable details for matters including, but not limited to, threshold transaction reports (**TTRs**). TTRs will be required to be submitted where a transfer of physical currency of A$10,000 or more (or the foreign currency equivalent) has occurred. As above, the intangible nature of digital currencies means that DCE providers are generally not required to make TTRs in connection with digital currency transactions. However, the rules associated with the AML/CTF Act set out specific details to be reported by DCE providers (such as digital currency type, value, description and relevant wallet addresses) in connection with TTRs, which may indicate scope for DCE providers to be caught by TTR obligations in the future. There are intentions for long-term reforms that should, among other things, clarify record-keeping requirements and reporting obligations for reporting entities following an AML/CTF statutory review in 2016; however, these have not yet been fully implemented.

Estate planning and testamentary succession

To date, there has been no explicit regulation or case law surrounding the treatment of cryptocurrency in Australian succession law. Generally, if estate plans do not cater for the specific nature of cryptocurrency and steps are not taken to ensure that executors can access a deceased's cryptocurrency (e.g., by accessing the private key), it may not pass to the beneficiaries.

A will should be drafted to give the executor authority to deal with digital assets. It may be helpful to select an executor with some knowledge of or familiarity with cryptocurrencies. As cryptocurrencies are generally held anonymously, a will should also establish the existence of the cryptocurrency (e.g., by identifying and cataloguing the relevant cryptocurrency) as an asset to be distributed to beneficiaries. A method must also be established to ensure that passwords to digital wallets and external drives storing cryptocurrency are accessible by a trusted representative. Unlike a bank account, which can be frozen or have access restrictions placed upon death, anyone can access a digital wallet, so care should be taken to ensure that external drives and passwords are not easily accessible on the face of the will. This may include providing a memorandum of passwords and accounts to the executor to be placed in a safe custody facility that remains unopened until a will is called upon.

There may also be tax implications arising for the beneficiaries of cryptocurrencies, which are similar to the tax implications for cryptocurrency holders. See "Taxation" above for further details.

Peter Reeves
Tel: +61 2 9263 4290 / Email: preeves@gtlaw.com.au

Peter Reeves is a partner at Gilbert + Tobin and leads the Fintech and Web3 team. He is an expert and market-leading practitioner in fintech and financial services regulation. Peter advises domestic and offshore corporates, financial institutions, funds, managers and other market participants in relation to establishing, structuring and operating financial services sector businesses in Australia. He also advises across a range of issues relevant to the fintech and digital sectors, including platform structuring and establishment, payments, blockchain solutions and digital asset strategies. *Chambers and Partners 2023* ranks Peter in Band 1 for Fintech and Peter is also ranked by *Chambers and Partners 2023* for Financial Services Regulation. Peter is recognised by *The Legal 500 2023* as a Leading Individual for Fintech + Financial Services Regulatory, *Best Lawyers 2023* in the area of Funds Management and as a top practitioner at the 2022 *FT* Innovative Awards.

Robert O'Grady
Tel: +61 2 9263 4241 / Email: raogrady@gtlaw.com.au

Robert O'Grady is a lawyer in G + T's Tech + IP group with a focus on fintech, payments, cryptocurrencies, blockchain, digital platforms, financial services regulation, funds establishment and management, credit, anti-money laundering and counter-terrorism financing regulation, and technology. Robert has specialist expertise and experience across a range of fintech and digital sectors, including digital platform and markets structuring, establishment and management, payments systems, infrastructure and ecosystems, bespoke digital asset and tokenisation implementation, blockchain applications, challenger lenders and neobanks.

Emily Shen
Tel: +61 2 9263 4402 / Email: eshen@gtlaw.com.au

Emily Shen is a lawyer in G + T's Tech + IP group with a focus on fintech, crypto and web3 and financial services regulation. She has advised a range of clients across the financial services, fintech and digital sectors on issues relating to payment and blockchain solutions, DeFi, crypto and other tokenisation deployments, DAOs, financial services regulation, digital and marketplace platforms, consumer credit and BNPL, neobank and purchased payment facility regulation, AML/CTF and funds establishment and structuring.

Gilbert + Tobin

Level 35, Tower Two, International Towers Sydney, 200 Barangaroo Avenue,
Barangaroo, Sydney NSW 2000, Australia
Tel: +61 2 9263 4000 / URL: www.gtlaw.com.au

Austria

Ursula Rath, Thomas Kulnigg & Dominik Tyrybon
Schönherr Rechtsanwälte GmbH

Government attitude and definition

Austrian financial regulators and policymakers are generally receptive to digital assets, new technologies and fintech.

The Austrian government closely monitors developments and continues to foster new technologies such as blockchain, distributed ledger technology and digital assets. While initial coin offerings ("ICOs"), initial token offerings ("ITOs"), security token offerings and initial exchange offerings seem to have slowed down significantly in recent years, we have noticed an uptick in innovative digital business models across a wide range of industries, especially in the mobile payments services sector, and more generally in platform-based crowdfunding/investment offerings, DeFi applications, non-fungible tokens ("NFTs") and open AI solutions.

In addition to its dedicated fintech contact point, the Austrian Financial Market Authority (*Finanzmarktaufsicht*; "FMA") established a regulatory sandbox in fall 2020 to assist with new business models requiring authorisation under Austrian financial services regulation (see further below). At the same time, regulators and the government stress that integrity, security and investor protection must not be compromised. While Austrian law does not prohibit cryptocurrencies, the FMA has warned investors of the risks of cryptocurrencies, stating that virtual currencies like Bitcoin and trading platforms for such instruments are neither regulated nor supervised by the FMA. Furthermore, the FMA is increasingly monitoring anti-money laundering ("AML") compliance and tightening requirements for (successful) registration as a virtual asset service provider ("VASP") with the FMA.

While national initiatives in this field are welcome, the issuance of and provision of services related to crypto-assets will, from mid-2024 onwards, be regulated on an EU-wide level: after long and intense debate among co-legislators, the final text of the Regulation on Markets in Crypto-assets ("MiCA") was finally adopted in April 2023.

MiCA will introduce a comprehensive (cross-border) regulatory framework for the offering and provision of services related to crypto-assets. It lays down (i) transparency and disclosure requirements for the issuance, offering to the public and admission to trading of crypto-assets on a trading platform for crypto-assets, (ii) authorisation requirements for crypto-asset service providers, issuers of asset-referenced tokens and issuers of electronic money tokens, and (iii) provisions for the operation, organisation and governance of crypto-asset service providers as well as crypto-asset issuers. In addition, and to foster integrity of crypto-asset markets, MiCA will introduce measures to prevent insider dealing, unlawful disclosure of inside information and market manipulation related to crypto-assets.

Cryptocurrency regulation

In Austria, cryptocurrencies initially caused quite a headache for financial market regulators, in particular as no statutory definition of cryptocurrencies existed at the time. While there is currently only one statutory definition of the term "virtual currency", defining virtual currencies for AML purposes as "*digital representation of value that is not issued or guaranteed by a central bank or a public authority, is not necessarily attached to a legally established currency and does not possess a legal status of currency or money, but is accepted by natural or legal persons as a means of exchange and which can be transferred, stored and traded electronically*", this has changed under MiCA: MiCA now defines "crypto-asset" broadly and in a technologically neutral way to capture all present and future types of assets that are not covered by any other financial services regulatory framework at EU level ("*a digital representation of a value or of a right that is able to be transferred and stored electronically using distributed ledger technology or similar technology*").

In addition, there are no dedicated cryptocurrencies or fintech-specific laws or regulations. From an Austrian financial services regulatory perspective, cryptocurrencies are currently neither treated as financial instruments (in particular, as securities or derivatives) nor as (fiat) currency (domestic or foreign), but as commodities. While commodities as such are not subject to supervision by the FMA, this does not mean that business activities involving cryptocurrencies are entirely outside the Austrian regulatory remit. For instance, derivatives referencing cryptocurrencies or tokens having certain features (i.e., security/investment tokens; see "Sales regulation", below) will qualify as financial instruments under MiFID II and will hence be covered by financial services regulation under MiFID II and the Markets in Financial Instruments Regulation.

More generally, depending on their specific features/content, the operation of business models based on cryptocurrencies may currently trigger licensing requirements under general financial services legislation (which also applies to cryptocurrencies and new business models/technologies) and/or fall within the remit of Austrian securities laws (see "Sales regulation", below). Based on the "same risk – same rules" principle, the FMA has always applied a "technology-neutral" supervisory approach to crypto-products and services. Whether and to what extent financial services regulation and securities laws apply depends primarily on the product features and business model. Business models involving crypto-assets may be subject to licensing requirements and are governed by:

- the Austrian Banking Act (*Bankwesengesetz*; "BWG") – for example, if funds are raised for investment into cryptocurrencies;
- the Austrian Payment Services Act 2018 (*Zahlungsdienstegesetz 2018*; "ZaDiG 2018") – for example, if information of several accounts is consolidated or if payments are initiated;
- the Securities Supervision Act 2018 – for example, if investment advice or portfolio management are provided in relation to financial instruments referencing cryptocurrencies or if orders are received and transmitted in relation to such instruments;
- the Austrian Alternative Investment Fund Managers Act (*Alternative Investmentfonds Manager-Gesetz*; "AIFMG") – for example, if funds are raised for investment into cryptocurrencies according to a pre-defined investment strategy, including for mining purposes; and
- the Electronic Money Act 2010 (*E-Geldgesetz 2010*) – when issuing electronic money.

Purely technical services do not require a licence. If, however, a technical billing service also included the transfer of fiat funds, this would no longer be considered a mere technical

service and would need to be tested against licensing requirements under Austrian financial services regulation.

Given the diversity, complexity and rapid evolution of business models, the regulatory treatment of any business models involving cryptocurrencies and crypto-assets must be assessed on a case-by-case basis. Therefore, the FMA encourages discussion of the regulatory treatment before engaging in any business activity. It has set up a dedicated specialist team and the fintech contact portal dedicated to those areas to handle all fintech-related queries and published guidance on the regulatory treatment of certain activities on its website at https://www.fma.gv.at/en/cross-sectoral-topics/fintech/fintech-navigator.

Sales regulation

There is currently no specific regulation dedicated to the sale of cryptocurrencies or tokens, which are thus covered by general securities and commodities laws.

Depending on an instrument's specific terms and conditions/features, certain token offerings/sales may be subject to prospectus requirements under Austrian securities laws unless a prospectus exemption applies.

For current Austrian supervisory law purposes, the FMA has broadly classified tokens as set out below, noting that, in practice, hybrid forms and overlaps frequently occur and that such classification is subject to any further national and international legal developments (some of which changed under MiCA; see below):

- *Security/investment tokens*: Tokens that represent assets, in particular payment claims against a specific issuer, e.g., to participate in future earnings or cash flows or tokens that represent membership rights within the meaning of corporate law. The design of such tokens is often similar to that of "classical securities", in particular bonds or shares. Security tokens are therefore frequently considered transferable securities pursuant to the EU Prospectus Regulation and the Austrian Securities Supervision Act. If a token is classified as a transferable security, this has far-reaching regulatory implications not only for the token issuer (as this may trigger prospectus requirements under European securities laws) but also for trading platforms on which such token is traded (as they will need to become authorised as stock exchanges or regulated trading venues) or custodial or wallet providers (as they will need to become authorised for safekeeping and administration), amongst others. Even if a security token does not classify as a transferable security (in particular because that token/coin is not transferable or its transfer is restricted), but provides access to capital or returns for a risk-sharing group of investors, it may classify as a "Capital Markets Act investment" and its offering may trigger national prospectus requirements similar to the EU Prospectus Regulation, unless a prospectus exemption applies.
- *Utility tokens*: While these are often comparable to vouchers, utility tokens occur in many different forms and also fulfil the function of payment tokens or security tokens (hybrid design), making their classification for supervisory law purposes rather difficult. If the token can only be used for designing a product or a service and is not otherwise associated with any claims, or if the token only grants access to a product or a service without simultaneously serving a payment purpose, then such token will not be covered by supervisory laws. If, on the other hand, the token may be redeemed at the issuer or other users of the platform for the use of a product or a service, then it rather fulfils a payment function similar to a payment token.

- *Payment/currency tokens*: Tokens that are accepted as means of payment for the purchase of goods or services, or tokens that serve the purpose of transferring money and value but do not confer any claims against a specific issuer (e.g., Bitcoin or Ripple).

Accordingly, due to their specific content/features, security/investment tokens will typically be subject to prospectus requirements (unless an exemption applies), while other types of tokens, such as utility tokens or payment/currency tokens, usually will not. Besides issuers, platform operators may also have the obligation to publish a prospectus, as they may be considered "offerors" for these instruments under the EU Prospectus Regulation. Breaches of the obligation to publish a prospectus are subject to severe sanctions, including under criminal laws.

MiCA affects the historic utility/payment token classification set out above, as it divides crypto-assets that are not MiFID financial instruments into the following sub-categories: (i) asset-referenced token ("ART"); (ii) electronic money token or e-money token ("EMT") covering stablecoins in particular; and (iii) crypto-assets other than ART or EMT, including utility tokens but also Bitcoin. Also, issuers and offerors may need to become authorised and prepare a specific disclosure document ("whitepaper" or "prospectus light") for offering crypto-assets in the EU, unless an exemption applies.

Taxation

Income tax treatment of cryptocurrencies

Pursuant to Section 27a para. 1 Income Tax Act, income from cryptocurrency holdings (including both current income and profit from disposals) is subject to a special tax rate of 27.5%, and does not count towards the progressive thresholds for the taxation of other income. This provision applies irrespective of whether the amount of tax due is withheld at source (i.e., as capital gains tax), or determined on the basis of the annual income tax return and/or assessment procedure. Since 1 March 2022, Austrian income tax law has provided a definition of "cryptocurrencies" for which this new income taxation is applicable. According to the Income Tax Act, a cryptocurrency is defined "*as a digital representation of value that is not issued or guaranteed by any central bank or public authority and is not necessarily pegged to a legally established currency and does not have the legal status of currency or money but is accepted by natural or legal persons as a medium of exchange and can be transmitted, stored and traded electronically*".

However, an exemption does apply to income from private loans made in cryptocurrency, provided that the transfer contracts underpinning the loan are available to the general public. Income from such private loans is counted towards the progressive income tax thresholds.

Compensation of losses

According to Austria's general tax regulations, profits and losses associated with income from cryptocurrencies can be calculated for tax purposes together with the profits and losses associated with other capital income, such as dividends or proceeds from disposing of shares. Special provisions for the set off of losses exist.

Commercial income

In principle, the special tax rate for cryptocurrencies applies to commercial assets as well as to traditional capital assets. However, the special rate does not apply if generating income from cryptocurrencies is part of the core activity of the business concerned. In particular, this means it does not apply to businesses trading commercially in cryptocurrencies, or to

businesses mining currency on a commercial basis. Gains from such activities are taxed, according to the progressive income tax thresholds, up to 55% income tax for individuals or (flat) corporate income tax of 25% (from 2023: 24%; and from 2024: 23%) for corporations.

Capital gains tax

Domestic (Austrian) taxable persons and service providers will be required to deduct Austrian withholding tax ("KESt") from capital income accrued after 31 December 2023. Until this date, the deduction of capital gains tax can be carried out on a voluntary basis. If income from cryptocurrencies was generated prior to 31 December 2023 and no voluntary withholding tax deduction was made, there is an obligation to include this income in the annual income tax return.

VAT treatment of cryptocurrencies

The exchange of cryptocurrencies (e.g., Bitcoin) into fiat currency (e.g., Euro) and *vice versa* is VAT-exempt (CJEU 22 October 2015, C-264/14, *Hedqvist*; VAT guidelines para. 759). Bitcoin mining as such is not subject to VAT because the recipient of the mining services cannot be determined (CJEU 22 October 2015, C-264/14, *Hedqvist*; VAT guidelines para. 759).

Purchases/supplies of goods or services that are subject to VAT, and which are paid for in cryptocurrency, are treated no differently from payments with fiat currency. The assessment basis for transactions subject to VAT is the fair market value of the units.

Money transmission laws and anti-money laundering requirements

As stated above, money transmission laws may apply to certain business activities involving cryptocurrencies. Cryptocurrencies and tokens used as means of payment may trigger a licensing requirement if they are intended for payment at third parties, and the network within which they can be used to purchase goods/services is large in terms of geographical reach, type of products/services and/or number of accepting parties. Also, if accounts are operated in connection with currencies, payment instruments or means of payment through which payments are made, the entity holding such accounts may need to become licensed as a payment service provider.

In addition, any activities involving cryptocurrencies are subject to AML requirements (including know-your-customer ("KYC") checks and AML prevention systems) if they:

- require a licence under financial services regulation (e.g., as provision of payment services); or
- are subject to AML requirements under commercial law. Pursuant to the Austrian Trade Code (*Gewerbeordnung*), commercial operators, including auctioneers, are subject to AML requirements if they make or receive cash payments of at least €10,000.

Moreover, certain providers of services concerning cryptocurrencies are currently subject to AML, KYC and customer due diligence requirements, reporting obligations and prior registration as VASPs with the FMA if they offer one or more of the following services:

- services to safeguard private cryptographic keys to hold, store and transfer virtual currencies on behalf of a customer (custodian wallets);
- exchanging virtual currencies into fiat currencies and *vice versa*;
- exchanging one or more virtual currencies into each other;
- transferring virtual currencies; and
- the provision of financial services for the issuing and selling of virtual currencies.

Under MiCA, the provision of services related to crypto-assets will become subject to prior authorisation and supervisory oversight. The list of licensable services largely mirrors the list of MiFID II investment services. Similarly, crypto-asset service providers authorised under MiCA will be able to passport services across the EU, which will eliminate one of the major obstacles faced by providers so far. However, only legal entities established in the EU may become authorised under MiCA and may hence provide crypto-asset services to European customers.

Promotion and testing

True to the government's motto "advice instead of punishment", the Austrian Ministry of Finance has implemented a dedicated regulatory sandbox programme that went live in fall 2020. In such a sandbox, companies that require a financial services licence will be able to swiftly and comprehensively clarify regulatory requirements for innovative business models in constant dialogue with the regulator and, if necessary, test such business model based on a scaled-down licence. The selection criteria for admission to the sandbox and further details are based on international best practice. Further information is available here: https://www.fma.gv.at/en/fintech-point-of-contact-sandbox/fma-sandbox.

Ownership and licensing requirements

Cryptocurrencies are currently treated by the Austrian regulator as commodities for supervisory law purposes (see "Cryptocurrency regulation", above). Applicable law as well as internal investment policies may restrict investment managers of certain investors to own cryptocurrencies for investment purposes. For example, Undertakings for the Collective Investment in Transferable Securities ("UCITS") funds, real estate investment funds pursuant to the Austrian Real Estate Investment Funds Act, or staff provision funds and their managers, may not invest in commodities. Pension funds and insurance companies are subject to qualitative and quantitative investment restrictions that will typically not permit direct investment into cryptocurrencies. Depending on the relevant investment policy, AIFs and their managers may, however, invest in cryptocurrencies.

There are currently no specific licensing requirements imposed on an investment advisor or fund manager holding cryptocurrency, over and above those set out under the general trade law/financial services licensing framework.

Mining

Mining Bitcoin and other cryptocurrencies as such is not yet regulated and is thus currently permitted. However, raising capital from the public in order to invest proceeds into mining of cryptocurrencies may be regulated (see "Cryptocurrency regulation" and "Sales regulation", above).

Border restrictions and declaration

There are currently no border restrictions or obligations to declare cryptocurrency holdings.

Reporting requirements

There are currently no reporting requirements for cryptocurrency payments made in excess of a certain value under Austrian law.

Estate planning and testamentary succession

There are no specific rules as to how cryptocurrencies are treated for purposes of estate planning and testamentary succession. Accordingly, general civil law rules apply. Cryptocurrencies qualify as (intangible) assets (*unkörperliche Sache*) for civil law purposes and as such can be included in estate planning/testamentary succession, or form part of a deceased person's estate.

Ursula Rath
Tel: +43 1 534 37 50412 / Email: u.rath@schoenherr.eu

Ursula Rath is a partner at Schoenherr in its Vienna office, where she specialises in financial services regulation, capital markets, financings and M&A transactions involving the financial services sector. For over a decade, she has advised issuers, selling shareholders, financial institutions and investors on a wide range of equity and debt capital markets transactions, disclosure requirements, inbound and outbound financial services, conduct of business requirements and compliance. She covers the full range of asset management and investment fund work and has advised clients on regulatory changes, such as under CRD IV/V, CRR/CRR II, PSD II or MiFID II or on Brexit contingency planning. As a renowned regulatory expert, Ursula serves as a member of the Regulatory Sandbox Advisory Board of the Austrian Ministry of Finance, where she consults on priority actions around innovative business models, start-up financing and digital assets. She was a founding member of blockchain think tank "thinkBLOCKtank", a Luxembourg-based, non-profit organisation, bringing together some of the most respected blockchain and distributed ledger experts, and regularly publishes on financial services regulation, capital markets and funds.

Thomas Kulnigg
Tel: +43 1 534 37 50757 / Email: t.kulnigg@schoenherr.eu

Thomas Kulnigg is a partner at Schoenherr, where he specialises in venture capital transactions and start-ups as well as technology transactions. Thomas also leads Schoenherr's technology & digitalisation group (https://www.schoenherr.eu/technology-digitalisation) and heads the firm's venture capital and start-up practice.

He was a founding member of think tank "thinkBLOCKtank", a Luxembourg-based, non-profit organisation, bringing together some of the most respected blockchain and distributed ledger experts, and is a member of the advisory board of the Digital Asset Association Austria (https://daaa.at).

Dominik Tyrybon
Tel: +43 1 534 37 50327 / Email: d.tyrybon@schoenherr.eu

Dominik Tyrybon has been an associate with Schoenherr since 2020. Dominik's main areas of practice are M&A, start-ups, venture capital, FinTech and blockchain matters. Dominik graduated from the University of Vienna (*Mag. iur.* 2018). Before joining Schoenherr, Vienna, he practised with an international law firm as an associate and legal advisor to a blockchain start-up. He is an active crypto investor and regularly publishes on issues relating to crypto regulation.

Schönherr Rechtsanwälte GmbH

Schottenring 19, 1010 Vienna, Austria
Tel: +43 1 534 37 0 / URL: www.schoenherr.eu

Bermuda

Steven Rees Davies, Charissa Ball & Alexandra Fox
Carey Olsen

Government attitude and definition

Bermuda has been recognised as a global leader in the regulation of blockchain and cryptocurrency-based services and related activities. The Bermuda government has pioneered one of the world's first comprehensive regulatory frameworks specifically designed to provide legal and regulatory certainty to industry participants whilst ensuring that business in the sector is conducted in accordance with the highest international standards.

The framework comprises two legislative arms that treat all cryptocurrencies, digital coins and tokens as the same for regulatory purposes and use the term "digital assets" to identify them all. The Digital Asset Business Act (**DABA**) introduced a licensing regime for businesses seeking to conduct "digital asset business" (defined below) whilst the Digital Asset Issuance Act (**DAIA**) introduced a regime to regulate persons seeking to carry on a "digital asset issuance" (defined below).

The Bermuda government also introduced an Insurtech Sandbox as an additional licensing regime designed to promote innovation in the use of technology in the insurance and reinsurance sectors. Effective 2023, the government has widened the scope of the Sandbox regime to encompass investment business to promote the offering of innovative products and testing of new technologies and delivery methods. Bermuda undertakings can now apply for the "test" licence under the Investment Business Act 2003 pursuant to which a person may carry on one or more investment activities within the controlled environment of the Bermuda Monetary Authority's (**BMA**) general regulatory sandbox, and may offer innovative products and test new technologies and delivery methods in such a manner as agreed with the BMA. Bermuda also introduced one of the world's first digital asset business bank licensing regimes that provides for a banking licence to be issued to persons seeking to provide traditional banking services to the digital asset sector. Jewel Bank is the first bank to be issued a DABA and banking licence under the regime.

The Bermuda government has announced that it will be launching a blockchain-based stimulus token for use in Bermuda's retail market and which will be a Bermuda dollar-backed stablecoin using technology developed by one of the first companies to be regulated under the DABA in Bermuda. The government has also been working on numerous other technology projects to further enhance the island's digital infrastructure, including the development of a digital ID system that meets internationally recognised standards of both privacy and anti-money laundering and anti-terrorist financing (**AML/ATF**) regulation and the introduction of submarine cabling legislation to protect both the environment surrounding the island and the submarine cables themselves that are the core infrastructure supporting the digital asset sector.

Bermuda has developed a collaborative business culture that involves government and industry working together to create opportunity and commercial success with a truly independent, actively engaged and globally recognised regulator maintaining the balance between the promotion of innovation and adherence to worldwide standards of regulation, compliance and transparency.

The BMA, as Bermuda's financial sector regulator, is a member of the Global Financial Innovation Network (**GFIN**) and also a member of the GFIN Coordination Group. GFIN was created to provide an efficient mechanism for innovators to interact with regulators and assist in navigating between jurisdictions as they look to scale and test new products and services. GFIN also provides a means for regulators to cooperate and share knowledge and experience in working with new and innovative product and service lines.

Cryptocurrency regulation

Digital Asset Business Act

Since the DABA became law in 2018, the BMA has continued to promulgate and update rules, regulations, codes of practice, statements of principles and guidance in order to supplement the DABA, with the result that the DABA operates in a similar manner to the regulatory frameworks in place for other financial services regulated by the BMA. In summary, the DABA specifies the digital asset-related activities to which it applies, imposes a licensing requirement on any person carrying on any of those activities, lays out the criteria a person must meet before it can obtain a licence, imposes (and permits the BMA to impose) certain continuing obligations on any holder of a licence, and grants to the BMA supervisory and enforcement powers over regulated digital asset businesses. The BMA and other industry stakeholders are constantly reviewing and monitoring the framework to ensure that it remains fit for purpose and meets with all international standards of regulation, compliance and transparency. Through consultation with industry, the BMA, together with the Bermuda government, has already updated and improved the provisions of the DABA to give greater clarity and to facilitate more effective administration of its provisions, evidencing an actively engaged and responsive regulator.

Scope of the DABA

The DABA applies to any entity incorporated or formed in Bermuda and carrying on digital asset business (irrespective of the location from which the activity is carried out) and to any entity incorporated or formed outside of Bermuda and carrying on digital asset business in or from within Bermuda.

A "digital asset" is defined as anything that exists in binary format and comes with the right to use it, and includes a digital representation of value that is (a) used as a medium of exchange, unit of account, or store of value and is not legal tender, whether or not denominated in legal tender, (b) intended to represent assets such as debt or equity in the promoter, (c) otherwise intended to represent any assets or rights associated with such assets, or (d) intended to provide access to an application of service or product by means of distributed ledger technology.

"Digital asset business" is defined as the provision of the following activities to the general public as a business:

- Issuing, selling or redeeming virtual coins, tokens or any other form of digital asset: this is intended to regulate any person providing these services to other persons, whether such other person is situated in or outside Bermuda. It does not include a digital asset issuance to fund an issuer's or promoter's own business or project, which is regulated under the DAIA (see below).

- Operating as a payment service provider business utilising digital assets, which includes the provision of services for the transfer of funds: the term "payment service provider" is used globally in AML/ATF laws, regulations and guidance, and is defined in Bermuda's Proceeds of Crime (Anti-Money Laundering and Anti-Terrorist Financing) Amendment Regulations 2010 as "a person whose business includes the provision of services for the transfer of funds".
- Operating as a digital asset exchange: this means the operation of a centralised or decentralised electronic marketplace used for digital asset issuances, distributions, conversions and trades, including primary and secondary distributions, with or without payment.
- Carrying on digital asset trust services: this means the carrying on of the business of acting as a fiduciary, agent, or trustee on behalf of another person for the purpose of administration and management of a digital asset.
- Providing custodial wallet services: this means the provision of services of storing or maintaining digital assets or a virtual wallet on behalf of a client.
- Operating as a digital asset derivative exchange provider: this means the operation of a centralised or decentralised marketplace used for digital asset derivative issuances, distributions and trades with or without payment and that provides the services of creating, selling or otherwise entering into digital asset derivatives contracts or clearing and settlement of the same.
- Operating as a digital asset services vendor: this includes a person that, under an agreement as part of its business, can undertake a digital asset transaction on behalf of another person or has power of attorney over another person's digital asset, or a person who operates as a market maker for digital assets, or a person who operates as a digital asset benchmark administrator. The definition is intended to be widely interpreted to include any other business providing specific digital asset-related services to the public, which at this time includes the borrowing and lending of digital assets as a business.
- Operating as a digital asset lending or digital asset repurchase transaction service provider: this includes (a) a person facilitating, either as principal or agent, digital asset lending transactions by which a counterparty transfers or lends digital assets to a borrower subject to commitment that the borrower will return equivalent digital assets with or without interest or premium on a future date or when requested to do so by the lender, and (b) a person facilitating, either as principal or agent, digital asset repurchase transactions by which a person transfers digital assets to a counterparty subject to a commitment to repurchase such digital assets or substituted digital assets of the same description from that counterparty at a specified price with or without premium on a future date specified or to be specified.

In addition to the above categories, the DABA includes an option for the Minister of Finance, after consultation with the BMA, to be able to add new categories or to amend, suspend or delete any of the categories listed above by order.

Licensing requirement

The DABA requires persons carrying on digital asset business to obtain a licence before doing so, unless that person is subject to an exemption order issued by the Minister of Finance. At the time of writing, the Minister has issued only one exemption order (BR/2023), which exempts: (i) the BMA; (ii) the Bermuda government and any entity owned by it; and (iii) any public authority, from requiring a licence to carry on digital asset business under section 10 of the DABA, and stipulates that the following non-specified persons shall notify the BMA of their intention to be exempt from the requirement to obtain a licence under section 10 of the DABA:

- a person providing an affinity or rewards programme, where value is granted as part of such programme, which value cannot be taken from or exchanged with the person for legal tender, bank credit or any digital asset;
- a publisher issuing, either himself or via another person on his behalf, a digital representation of value, which is used exclusively within an online game, game platform, or family of games sold by the same publisher or offered on the same game platform;
- a person providing data storage or security services for a digital asset business, but is not otherwise engaged in digital asset business activity on behalf of other persons;
- an undertaking providing digital asset business activity solely for the purpose of its business operations or the business operations of any group undertaking; and
- an investment fund that has appointed an investment manager that is licensed under the Investment Business Act 2003, or authorised by a recognised regulator, as such term is defined under section 2 of the Investment Business Act 2003.

The foregoing non-specified persons will be required to file an annual declaration to the BMA stating that they continue to qualify for the exemption.

Three classes of licence are available for applicants:

- a Class F licence is a full licence to conduct any or all digital asset business activities and is not subject to a specified period, although the BMA has discretion to make any licence subject to restrictions where it deems it appropriate in the circumstances;
- a Class M licence is the same as a Class F licence except with modified requirements and restrictions and will only be valid for a specified period of time determined by the BMA on a case-by-case basis; and
- a Class T licence is for the sole purpose of carrying out pilot or beta testing in relation to the applicable digital asset business activities.

The intention behind this tiered licensing regime is to allow start-ups engaging in digital asset business to do so in a properly supervised regulatory environment, and to engage in proof of concept and develop a track record before obtaining a modified or full licence. The modified licence allows for persons who have developed proof of concept and are seeking to launch their products and services into the market but might not yet be able to meet all the requirements of a full licence. The restrictions to which a licensee will be subject will depend on the business model of the prospective licensee and the risks associated with it, but include an obligation to disclose to prospective customers the fact that the licensee holds either a Class T or Class M licence and certain limitations on the volume of business the licensee is permitted to conduct, along with other restrictions as the BMA may deem necessary or appropriate on a case-by-case basis.

A licence will further specify one or more of the eight categories of digital asset business activities that the licensee is permitted to conduct. Carrying on digital asset business without a licence is a criminal offence punishable by a fine of up to US$250,000, imprisonment for a term of up to five years, or both.

Application process

An application for a digital asset business licence is made to the BMA and must specify the class of licence being sought and be accompanied by (a) a business plan setting out the nature and scale of the digital asset activities to be conducted, (b) particulars of the applicant's arrangements for the management of the business, (c) policies and procedures to be adopted by the applicant to meet the obligations under the DABA and the Proceeds of Crime (Anti-Money Laundering and Anti-Terrorist Financing) Regulations 2008, (d) such other information and documents as the BMA may reasonably require for the purpose of determining the application, and (e) the applicable application fee.

Criteria to be met by licensees

The DABA provides that the BMA may not issue any licence unless it is satisfied that the applicant fulfils certain minimum criteria addressing the fitness and propriety of directors and officers, ensuring business is conducted in a prudent manner, the integrity and skill of the business's management, and standards of corporate governance observed by the (prospective) licensee. This is consistent with the position under other regulatory laws applicable to other sectors and is intended to ensure that the BMA maintains high standards for the conduct of regulated business. The BMA has also published a code of practice detailing requirements as to, *inter alia*, governance, risk management and internal controls applicable to licensees. The BMA recognises, however, that licensees have varying risk profiles arising from the nature, scale and complexity of the business, so assesses a licensee's compliance with this code in a proportionate manner relative to the business's nature, scale and complexity.

The DABA requires licensees to notify the BMA upon changes in directors or officers, and the BMA has powers to, *inter alia*, object to and prevent new or increased ownership of shareholder controllers and the power to remove controllers, directors and officers who are no longer fit and proper to carry on their role.

Continuing obligations of licence holders

Persons holding a licence issued under the DABA are subject to several ongoing obligations.

Client disclosure rules: the BMA has used powers conferred to it under the DABA to promulgate the Digital Asset Business (Client Disclosure) Rules 2018 in order to mitigate the high degree of risk for consumers owing to the highly speculative and volatile nature of digital assets. These rules require licensees, before entering any business relationship with a customer, to disclose to that customer: all material risks associated with its products, services and activities; and any additional disclosure the BMA may determine is reasonably necessary for the protection of clients. At the time of entering into an agreement with a client, a licensee must disclose: the class of licence it holds; a schedule of its fees and the manner in which fees will be calculated if not set in advance; whether it has insurance against loss of customer assets arising from being hacked or otherwise stolen; the extent to which a transfer or exchange of digital assets is irrevocable and any exceptions; governance or voting rights regarding client assets if the licensee is to hold client assets; the extent to which it will be liable for an unauthorised, mistaken or accidental transfer or exchange; and sundry other matters. The rules also oblige licensees to confirm certain information regarding transactions with clients at the conclusion of each such transaction.

Cybersecurity rules: alongside the client disclosure rules described above, the BMA has promulgated the Digital Asset Business (Cybersecurity) Rules 2018, which require licensees to file an annual cybersecurity report prepared by its chief information security officer assessing the availability, functionality and integrity of its electronic systems, any identified cyber risk arising from any digital asset business activity carried on or to be carried on by the licensee, and the cybersecurity program implemented and proposals for steps to remediate any inadequacies identified.

The cybersecurity program itself must include (but is not limited to) the following audit functions:

- penetration testing of its electronic systems and vulnerability assessment of those systems conducted at least on a quarterly basis; and
- audit trail systems that:
    - track and maintain data that allows for the complete and accurate reconstruction of all financial transactions and accounting;

- protect the integrity of data stored and maintained as part of the audit trail from alteration or tampering;
- protect the integrity of hardware from alteration or tampering, including by limiting electronic and physical access permissions to hardware and maintaining logs of physical access to hardware that allows for event reconstruction;
- log system events including, but not limited to, access and alterations made to the audit trail systems, and cybersecurity events; and
- maintain records produced as part of the audit trail.

In 2023, the BMA issued the Digital Asset Business (Cyber Risk) Rules 2023, which, effective on 1 January 2024, will supplant the Digital Asset Business (Cybersecurity) Rules 2018, and require Class F licence holders to file cyber risk returns with the BMA on an annual basis. Class M and Class T licence holders will be required to make such filing as often as prescribed by the BMA.

Custody and protection of consumer assets: licensees holding client assets are required to have in place and maintain a surety bond, trust account or indemnity insurance for the benefit of their customers, in such form and amount as the BMA deems acceptable or such other arrangements as the BMA may approve. Any such trust account must be maintained with a qualified custodian appropriate for the type of asset held. A licensee is, in addition, required to maintain books of account and other records sufficient to ensure that customer assets are kept segregated from those of the licensee and can be identified at any time. All customer funds must be held in a dedicated separate account and clearly identified as such.

Senior representative: the DABA imposes an obligation on licensees to appoint a senior representative, to be approved by the BMA, who must maintain an office in Bermuda (except where such representative is approved by the BMA for purposes of a Class T licence) and who is sufficiently knowledgeable about both the licensee itself and the industry in general. This senior representative will himself be under a duty to report to the BMA certain significant matters, including:

- failure of the licensee to comply with conditions, provisions or directions imposed by the BMA;
- involvement of the licensee in any criminal proceedings, whether in Bermuda or abroad;
- the licensee ceasing to carry on digital asset business in or from within Bermuda;
- a material change to the business of the licensee;
- a cyber reporting event; or
- the licensee ceasing to be eligible for an exemption from licensing under the Investment Business Act 2003, due to its investment business no longer qualifying as ancillary to the digital asset business for which it is licensed under the DABA.

Head office: the DABA also requires licensees, other than those issued a Class T licence, to maintain a head office in Bermuda and to direct and manage their digital asset business from Bermuda. The relevant section goes on to list several factors the BMA shall consider in determining whether a licensee satisfies this requirement, together with a number of additional factors to which the BMA may (but need not) have regard.

Annual prudential return: a licensee is obliged to file with the BMA an annual prudential return, with the BMA being granted the power to require more frequent filings or additions to a filing if required in the interest of consumer protection. The annual prudential return should be accompanied by a copy of the licensee's audited financial statements and business plan for the following year, and include information relating to, *inter alia*, business strategy

and risk appetite, products and services, the number, risk rating and geographical profile of customer accounts, information on risk and cybersecurity (including a risk self-assessment and policies in these areas), AML/ATF controls, corporate governance, audited financial statements and details on any outsourcing to third parties.

BMA's supervision and enforcement powers

The DABA grants the BMA wide-ranging powers of supervision and enforcement. It will have the power to compel production of information and documents (with criminal sanctions for non-production or for making false or misleading statements), the power to issue such directions as appear to be desirable to it for safeguarding the interests of a licensee's clients where a licensee is in breach of the DABA or regulations or rules applicable to it, and the power to impose conditions and restrictions on licences. For example, the BMA may:

- require a licensee to take certain steps or to refrain from adopting or pursuing a particular course of action, or to restrict the scope of its business activities in a particular way;
- impose limitations on the acceptance of business;
- prohibit a licensee from soliciting business, either generally or from prospective clients;
- prohibit a licensee from entering into any other transactions or class of transactions;
- require the removal of any officer or controller; and/or
- specify requirements to be fulfilled otherwise than by action taken by the licensee.

In more extreme cases, the BMA may revoke a licence altogether and, if it so elects, subsequently petition the court for the entity whose licence it has revoked to be wound up. In the event a licensee fails to comply with a condition, restriction or direction imposed by the BMA or with certain requirements of the DABA, the BMA has the power to impose fines of up to US$10,000,000. Alternatively, it may issue a public censure ("naming and shaming"), issue a prohibition order banning a person from performing certain functions for a Bermuda regulated entity, or obtain an injunction from the court. The BMA will use these enforcement powers in a manner consistent with the Statement of Principles and Guidance on the Exercise of Enforcement Powers it published in September 2018, which contains general guidance applicable to all regulated sectors on the BMA's approach to the use of its enforcement powers and the factors it will consider in assessing whether to exercise those powers.

Digital Asset Issuance Act

The DAIA came into force in May 2020, superseding legislation that had been introduced in 2018 to initially regulate persons carrying on an offering of digital assets via a digital asset issuance in or from within Bermuda and to protect the interests of persons acquiring digital assets through such issuances. Since the DAIA's enactment, the BMA has continued to promulgate rules and a statement of principles in order to supplement the DAIA. In summary, the DAIA specifies what activities amount to a digital asset issuance, prohibits such activities other than by authorised undertakings, lays out the criteria a person must meet before it can become an authorised undertaking, imposes (and permits the BMA to impose) certain continuing obligations on any authorised undertaking, and grants to the BMA supervisory and enforcement powers over the issuers and/or promoters of digital asset issuances. The BMA and other industry stakeholders are constantly reviewing and monitoring the framework to ensure that it remains fit for purpose and meets with all international standards of regulation, compliance and transparency. Through consultation with industry, the BMA, together with the Bermuda government, has already updated and improved the provisions of the DAIA to give greater clarity and to facilitate more effective administration of its provisions, evidencing an actively engaged and responsive regulator.

Scope of the DAIA

The DAIA applies to any undertaking incorporated or formed in or outside Bermuda and that conducts any digital asset issuance in or from within Bermuda. A "digital asset issuance" is defined as an offer to the public, or any section of the public, to acquire digital assets or to enter into an agreement to acquire digital assets at a future date. The DAIA requires any undertaking seeking to conduct a digital asset issuance to obtain prior authorisation from the BMA.

If the digital asset issuance would not result in the digital assets becoming available to more than 150 persons or was to persons whose ordinary business involves the acquisition, disposal or holding of digital assets or was an offer to qualified acquirers, then the undertaking conducting such digital asset issuance would not be treated as an offer to the public. In such instances, the issuer and/or promoter would be required to file a digital asset placement declaration form with the BMA prior to entering any transaction rather than having to seek prior authorisation. "Qualified acquirers" include high-income (US$200,000 *per annum* for two years) and high-net-worth (greater than US$1,000,000 excluding residence value) private acquirers, corporate and unincorporated bodies with not less than US$5,000,000 in assets and other similar persons and arrangements.

Conducting a digital asset issuance in or from within Bermuda without authorisation is a criminal offence punishable by a fine of up to US$100,000, imprisonment for a term of up to five years, or both.

Authorisation requirements

An application for authorisation to conduct a digital asset issuance shall be made to the BMA and be accompanied by (a) a business plan setting out the nature and scale of the digital asset issuance to be conducted, (b) a copy of the issuance document to be made available to digital asset acquirers, (c) particulars of the applicant's arrangements for the management of the offering via the issuance, (d) policies and procedures to be adopted by the applicant to meet the obligations under the DAIA and the Proceeds of Crime (Anti-Money Laundering and Anti-Terrorist Financing) Regulations 2008, (e) such other information and documents as the BMA may reasonably require for the purpose of determining the application, and (f) the applicable application fee.

Authorisation criteria

The DAIA provides that the BMA may not authorise an undertaking to conduct a digital asset issuance unless it is satisfied that the applicant fulfils certain minimum criteria addressing the fitness and propriety of directors and officers, ensuring business is conducted in a prudent manner, the integrity and skill of the business's management, and standards of corporate governance observed by the undertaking. This is consistent with the position under other regulatory laws applicable to other sectors and is intended to ensure the BMA maintains high standards for the conduct of regulated business. The BMA has also published the Digital Asset Issuance Rules 2020 (**Rules**), detailing requirements as to, *inter alia*, minimum required information for a digital asset issuance document, ongoing disclosures and information technology and cybersecurity, custody of acquirer assets and compliance measures.

The DABA requires licensees to notify the BMA upon changes in directors or officers, and the BMA has powers to, *inter alia*, object to and prevent new or increased ownership of shareholder controllers and the power to remove controllers, directors and officers who are no longer fit and proper to carry on their role.

Ongoing obligations

Authorised undertakings are subject to several ongoing obligations.

Communications facility: the promoter shall provide during the period of an offer, or suspension, an electronic facility for persons to access the issuance document, post and read messages relating to the offer and ask questions relating to the offer.

Cooling-off rights: provide a mechanism through which any applicant that has agreed to acquire digital assets under the offering to withdraw the application within three business days after the application is made.

Information technology and cybersecurity rules: an authorised undertaking is under an obligation to establish and maintain, for the duration of its authorisation and five years beyond, a data audit node in Bermuda where all information about the digital asset issuance will be stored real-time in an accurate and tamper-proof manner as well as deliver a cybersecurity report and program similar to those required under the DABA (see above).

Custody and separate accounts: an authorised undertaking holding the assets of digital asset acquirers shall keep its accounts in respect of such assets separate from any accounts kept in respect of any other business for a period of time as specified in the legislation and Rules.

Local representative: authorised undertakings must appoint a local representative, to be approved by the BMA, who must maintain an office in Bermuda and who is sufficiently knowledgeable about both the authorised undertaking itself and the industry in general. This local representative will be under a duty to report to the BMA certain significant matters, including: a likelihood of the licensee becoming insolvent; breaches by the authorised undertaking of any conditions imposed by the BMA; involvement of the licensee in criminal proceedings, whether in Bermuda or elsewhere; a material misstatement being found in the issuance document; and other material developments.

Compliance measures: an issuer shall ensure that it applies "appropriate measures" with regard to customer due diligence in relation to a digital asset issuance as set out in the Rules as well as appoint a Reporting Officer and Compliance Officer.

BMA's supervision and enforcement powers

The DAIA grants the BMA wide-ranging powers of supervision and enforcement similar to those granted under the DABA (see above).

Sales regulation

Other than the digital asset business activity of issuing, selling or redeeming of digital assets under the DABA and the offering of digital assets by way of an issuance under the DAIA, there are no Bermudian laws, regulations or other restrictions governing the participation of persons resident or situated in Bermuda in the purchase, holding or sale of digital assets, unless such digital assets represent an interest in a security in a Bermuda company to which the Exchange Control Act and related regulations may apply. Further, digital assets that purport to represent an interest in real property, vessels, aircraft or engines situated or registered in Bermuda may also be subject to legislation and regulation applicable to such underlying assets.

Taxation

There are no income, capital gains, withholding or other taxes imposed in Bermuda on digital assets or on any transactions involving them (the potential application of Bermuda's foreign currency purchase tax is discussed below, under "Border restrictions and declaration").

Moreover, exempted companies or limited liability companies carrying on digital asset business, including digital asset issuers, may apply for an undertaking from the Minister of Finance to the effect that, in the event of there being enacted in Bermuda any legislation imposing tax computed on profits or income or computed on any capital asset, gain or appreciation, then the imposition of any such tax shall not be applicable to such company or to any of its operations.

Money transmission laws and anti-money laundering requirements

Operating a payment service business utilising digital assets (including the provision of services for the transfer of funds) or operating a digital asset exchange constitutes a regulated activity for the purposes of the DABA (on which see above).

Bermuda has a long-established and well-earned reputation as an international financial centre, and a crucial aspect of this is its robust AML/ATF regime. The jurisdiction made further enhancements to this regime ahead of its fourth-round mutual evaluation by the Financial Action Task Force in 2018.

The DABA amended certain provisions of Bermuda's existing AML/ATF laws and regulations to ensure that the AML/ATF regime applies expressly to the carrying on of digital asset business. The BMA has since published its "Sector-Specific Guidance Notes on Anti-Money Laundering and Anti-Terrorist Financing for Digital Asset Business", which enhance the main guidance notes for AML/ATF regulated financial institutions. The BMA has also recently updated the main guidance notes for AML/ATF following a consultation with industry stakeholders.

A detailed discussion of the requirements imposed by Bermuda's AML/ATF regime is beyond the scope of this chapter, but in short, digital asset businesses are required to establish policies and procedures to prevent money laundering and terrorist financing. These policies and procedures must cover customer due diligence, ongoing monitoring, reporting of suspicious transactions, record-keeping, internal controls, risk assessment and management, and the monitoring and management of compliance with, and internal communication of, these policies and procedures.

Promotion and testing

The Bermuda government has launched and continues to develop a number of initiatives aimed at promoting research and investment in technology, including blockchain, in Bermuda. The Class T licence under the DABA, the Insurtech Sandbox regime and the "test" licence available under the Investment Business Act 2003, which allow for the testing and development of technology or technologically driven products and services in a safe and cooperative regulatory environment, are just two examples.

The Bermuda government has also appointed a specialist technology team with a remit to promote the sector in Bermuda and attract more business to the island. The team also provides a specialist concierge service aimed at making the transition to Bermuda as easy as possible for new entrants.

The Bermuda government has also introduced a tailored immigration policy for technology businesses that provides technology-focused companies that are new to Bermuda to seek immediate approval of work permits for non-Bermudian staff. To benefit from this, a business must present a plan for the hiring, training and development of Bermudians in entry-level or trainee positions. A business may not, however, apply for a work permit

under this policy in respect of any job categories that are closed (i.e. reserved exclusively for Bermudians, their spouses and permanent resident certificate holders only) or restricted (in respect of which a permit may only be obtained for one year) under Bermuda's employment legislation, or which are entry-level, graduate or trainee positions.

Ownership and licensing requirements

Under current Bermuda law, and under the DABA and DAIA, no licensing requirements are imposed on any person merely by virtue of that person holding any form of digital asset, unless that person does so in the course of its business and on behalf of another, in which case that person will likely be regarded as either a digital asset trust services provider or a digital asset services vendor and thus subject to regulation under the DABA.

An investment fund incorporated or formed in Bermuda that proposes to deal in digital assets as part of its investment strategy may fall within the ambit of the Investment Funds Act 2006. Depending on the type of fund, an investment fund that has appointed an investment manager that is licensed under the Investment Business Act 2003 or authorised by a recognised regulator (as such term is defined under section 2 of the Investment Business Act 2003) will be exempt from licensing under the DABA under the Digital Asset Business Exemption Order 2023, provided an annual notice is filed with the BMA.

Mining

Digital asset mining is not within scope of the DABA and therefore remains an unregulated activity from a Bermuda perspective, whether conducted in Bermuda or by a Bermuda company outside of Bermuda. Notwithstanding this, the BMA is aware of other jurisdictions where such activity is prohibited or restricted in some way and will expect any Bermuda company conducting mining activity outside of Bermuda to be wholly compliant with any laws or regulations applied by the governing authorities of the jurisdictions where such activities are being conducted.

Border restrictions and declaration

Bermuda imposes a foreign currency purchase tax of 1% whenever a Bermuda resident purchases a foreign currency from a Bermuda-based bank. This tax will not apply to most (if not all) purchases of cryptocurrency or other digital assets, on the grounds that these are purchased almost exclusively from digital asset exchanges, whereas the foreign currency purchase tax applies only to purchases from banks in Bermuda. This renders immaterial the question of whether "foreign currency" in this context would include cryptocurrency (the BMA has not, to date, expressed a view).

There are no other border restrictions on cryptocurrencies or other digital assets; the only obligation to make a customs declaration in respect of any form of money arises in respect of cash or negotiable instruments in excess of US$10,000.

Reporting requirements

Digital asset businesses and their senior representatives are subject to certain reporting obligations under the DABA, as described in more detail above. The DABA does not impose any reporting requirements in respect of individual digital asset payments, irrespective of their value, although licensees are required to include anonymised details on transaction volume, value and geographical spread in their annual returns.

Estate planning and testamentary succession

There are no Bermuda laws that deal specifically with the treatment of cryptocurrencies or other digital assets upon the death of an individual holding them. This means that, in principle, digital assets will be treated in the same way as any other asset and may be bequeathed to beneficiaries in a will, or, if a person dies intestate, will fall to be dealt with under the Succession Act 1974.

The main potential difficulty that may arise is practical and is by no means unique to Bermuda; namely that anyone inheriting any kind of digital asset will, on the face of it, only be able to receive the rights to and value of the digital asset if the beneficiary has the private key relevant to the digital asset wallet through which the digital asset is held. Most exchanges have policies in place to transfer digital assets to next of kin but these policies, and the transfer requirements, will vary between the exchanges.

Steven Rees Davies
Tel: +1 441 705 8848 / Email: steven.reesdavies@careyolsen.com

Steven's practice covers a broad spectrum of corporate and commercial law with specific depth and experience in corporate governance, finance, securities, regulatory compliance, mergers and acquisitions and restructuring. A recognised specialist in the digital asset sector, Steven worked with the Bermuda government and other key stakeholders in the introduction and development of Bermuda's digital asset legal and regulatory regime, and represents a significant number of digital asset companies headquartered, or with operations, in Bermuda. He also has particular expertise in the wider technology, telecommunications and energy sectors with depth and experience in representing clients on local and cross-jurisdictional corporate and regulatory transactions and restructurings, including complex multinational joint ventures and public and private offerings.

Charissa Ball
Tel: +1 441 542 4276 / Email: charissa.ball@careyolsen.com

Charissa advises on all aspects of Bermuda commercial and corporate law, with a practice spanning a number of specialisations and particular experience in corporate reorganisations, mergers and acquisitions, debt restructuring, redomiciling, joint ventures and debt and equity offerings. She also has considerable experience in corporate finance including IPOs, private equity investments and banking, and financial services including financial derivatives, credit and security. In fintech, Charissa has assisted numerous digital asset business companies, including advising on the licensing and ongoing regulatory requirements of digital asset companies. Prior to joining Carey Olsen, Charissa practised as a corporate attorney with another law firm, working in its Bermuda, Hong Kong and Singapore offices, advising public and private international companies, investment banks, licensed financial institutions and family offices.

Alexandra Fox
Tel: +1 441 542 4265 / Email: alexandra.fox@careyolsen.com

Alexandra advises on all aspects of Bermuda corporate and commercial law, specialising in corporate finance and restructuring. She has also assisted with various fintech and insurtech matters, including advising on the licensing and ongoing regulatory requirements of digital asset companies and insurance intermediaries. Alexandra regularly assists corporate creditors and obligors on a variety of local and cross-jurisdictional transactions across a wide array of industries, including film and media, healthcare and pharmaceutical, tourism and hospitality, energy and natural resources, insurance and digital asset business.

Carey Olsen

Rosebank Centre, 5th Floor, 11 Bermudiana Road, Pembroke HM 08, Bermuda
Tel: +1 441 542 4500 / URL: www.careyolsen.com

Brazil

Luiz Felipe Maia, Flavio Augusto Picchi & André Napoli
Maia Yoshiyasu Advogados

Government attitude and definition

Government attitude

Over the past few years, several public authorities in Brazil, especially at the federal level, have expressed a positive view and great interest in the cryptoasset and blockchain industries, and a handful of regulations and public projects have emerged in connection to them ever since.

Most recently, after years of discussion in the legislative branch, the Brazilian virtual assets legal framework – Law No. 14,478/22[1] ("**Legal Framework for Virtual Assets**") – was finally enacted and entered into force on June 20, 2023. The Legal Framework for Virtual Assets focused on more general concepts and principles, and the Brazilian Central Bank (*Banco Central do Brasil* – "**BCB**") was designated the competent authority to effectively regulate, authorise and supervise the provision of services of virtual asset service providers ("**VASPs**") in Brazil, pursuant to Decree No. 11,563 of June 13, 2023.[2]

The edition of the rules by BCB is still pending and is expected by the end of 2023, after the holding of public consultations by the entity (announced on July 18, 2023),[3] in which all members of society will have the opportunity to present contributions to the forthcoming regulation. Nonetheless, even with the current regulatory gap, the Legal Framework for Virtual Assets itself represented an important milestone for the industry, as it consolidated the legality of the activities of VASPs, brought greater legal certainty for the sector and its players, and provided for certain rights and obligations with immediate effect, which will be further discussed in the "Cryptocurrency regulation" section below.

Moreover, at present, several public agencies – especially BCB – are proactively working to create their own projects and systems based on blockchain technology, in order to develop the efficiency of public administration and the financial system in Brazil.

Definition and historical background

The Brazilian Real ("**BRL**") has been the fiat currency in Brazil since 1994 and it has exclusive legal tender. Even though cryptocurrencies and other similar virtual assets may be privately used as payment methods, they are classified as goods or movable property. They are not considered money or equivalent to fiat currency.

Law No. 12,865/13[4] was enacted in October 2013 to regulate payment systems, and, among other provisions, adopted the concept of "*electronic money*" or "*electronic currency*", which was then defined as "*assets stored in electronic devices or electronic systems that allow the final user to perform a payment transaction*". A few months later, in February 2014, BCB issued Policy Statement No. 25,306/14[5] to raise awareness of the risks associated with

the acquisition and negotiation of so-called "*virtual currencies*" or "*encrypted currencies*", expressly stating that such assets were not encompassed under the concept of "*electronic money*" or "*electronic currency*" adopted by Law No. 12,865/13.

According to BCB, "*electronic money*" – as defined in Law No. 12,865/13 – refers to resources in BRL that are stored in electronic devices or systems that allow end users to perform payment transactions. Virtual (or encrypted) currencies, on the other hand, (i) were denominated in units of account unrelated to sovereign fiat currencies, (ii) could not be stored in devices or electronic systems in BRL, (iii) were not issued by, guaranteed by, or convertible into any sovereign currency issued by a monetary authority, and (iv) were not backed by real assets of any kind. In November 2017, BCB Policy Statement No. 31,379/17[6] reaffirmed this understanding and warned that (i) companies engaged in selling and storing cryptocurrencies on behalf of their users were not regulated or supervised by BCB (as BCB's competence to regulate and supervise VASPs was established only recently, on June 13, 2023), and (ii) engaging in activities involving cryptocurrencies would imply significant risk.

Cryptoassets were only first and more formally defined in May 2019, when the Federal Revenue Office (*Secretaria Especial da Receita Federal do Brasil* – "**RFB**") issued Normative Ruling No. 1,888/19, which is still in force, to establish reporting requirements for transactions involving such assets. According to RFB, a cryptoasset is the "*digital representation of value denominated in its own unit of account, the price of which can be expressed in local or foreign currency, traded electronically using cryptography and distributed registration technologies, used as a form of investment, value transfer instrument or access to services, and which is not recognized as a currency*". Crypto exchanges, in turn, are defined as "*legal entities, either engaged in financial activities or not, offering services with respect to cryptoasset transactions, including brokerage, negotiation or custody, and that may accept any means of payment, including other cryptoassets*". Apart from this ordinance, the current legislative scenario in relation to cryptoassets is further discussed in detail in the "Cryptocurrency regulation" section below.

Government applications

Several interesting projects are currently in development by public agencies, some of which are highlighted below.

BCB's LIFT

The Financial and Technological Innovations Laboratory (*Laboratório de Inovações Financeiras Tecnológicas* – "**LIFT**") was enacted in 2018 as a joint initiative of BCB and the National Federation of Associations of the Central Bank Employees (*Federação Nacional de Associações dos Servidores do Banco Central*).[7] LIFT's goal is to foster innovation within the National Financial System by encouraging the creation of prototypes of innovative technological solutions. So far, several blockchain-based projects have been developed and launched, such as a decentralised platform for recording credit rights, peer-to-peer lending systems, and a digital wallet specifically designed for tax payments.[8] In addition to its regular editions, LIFT also launched a special sandbox programme in November 2021 – the "LIFT Challenge Real Digital" ("**LIFT Challenge**")[9] – which was aimed specifically at the development of use cases for the "Real Digital", the Central Bank Digital Currency ("**CBDC**") currently in development in Brazil by BCB (discussed in detail in the "Real Digital" section below).

Recently, on April 25, 2023, BCB promoted the "LIFT Day 2023",[10] where LIFT-selected projects presented their results, prototypes and technical reports. The event presented both projects from the regular edition of LIFT 2022, which included microcredit themes, the

interoperability of Real Digital with other networks, and functionalities directed at PIX (a Brazilian original payment method), as well as specific projects from the LIFT Challenge, related to Real Digital, which featured projects regarding the purchase and selling of financial assets, non-financial assets and cryptoassets, and encompassed themes such as decentralised finance, international remittances, offline payments, and the internet of things ("**IoT**").

Real Digital

Perhaps the boldest initiative in Brazil so far is the adoption of a Brazilian CBDC by BCB – Real Digital, as mentioned above. After initial discussions carried out by a working group created in August 2020,[11] general guidelines for a Brazilian CBDC were released in May 2021,[12] and a sandbox programme to develop the currency was launched by LIFT through a special initiative, the aforementioned LIFT Challenge.[13] In summary, the LIFT Challenge intends to assess use cases of the digital currency, as well as its technological feasibility, and to develop minimum viable products. From 47 proposals originally submitted to LIFT, nine projects were selected, which are now in the process of development – for instance, a renowned Brazilian financial institution is designing a platform that allows the custody and exchange of currencies and alternative investments through blockchain and smart contracts. The use case consists of creating liquidity pools as in current decentralised finance systems, with tokens that emulate stablecoins in parity with the BRL, the US Dollar, or other fiat currencies.[14]

In February 2023, in light of the LIFT Challenge's results, BCB revised the Real Digital guidelines and, as of March 2023, started testing a platform for Real Digital operations, the "RD Pilot" (*Piloto RD*), whose final product will be a technological and commercial assessment report.[15] Discussions aim to reconcile a wide variety of use cases of Real Digital with the many institutional payment arrangements already in place in Brazil and the technologies available for its implementation. A few of the main new guidelines for Real Digital are, for example: (i) the emphasis on developing innovative models incorporating technologies such as smart contracts and programmable money, compatible with settlements through the IoT; (ii) developing online applications while considering the possibility of offline payments; and (iii) compliance with privacy and security principles and rules outlined in Brazilian legislation, especially in regard to banking secrecy and the protection of personal data, pursuant to Law No. 13,709/18 (the Brazilian General Data Protection Law). Most recently, in a movement of absolute transparency and aiming for societal discussion and collaboration, BCB has made public the current source code for Real Digital on the platform GitHub,[16] which has already led to several suggestions, questions and criticism of the project. As a result of such disclosure, it was brought to light – as further confirmed by BCB itself – that, as the CBDC is presently designed, BCB would have the capacity to issue, destroy, freeze in part or in full, or change the ownership of Real Digital from the account of its holders.[17]

TCU blockchain report

Finally, it is worthy of note that the Federal Court of Accounts (*Tribunal de Contas da União* – "**TCU**"), which is the federal government's external control agency, published an extensive and detailed report in August 2020 on the potential advantages of adopting blockchain and distributed ledger technologies in public administration.[18]

Outlook

On June 21, 2023, a few days after the publication of Decree No. 11,563/23, which established BCB's competence to regulate and supervise the sector, the entity issued a public note stating that it had been studying and closely following the virtual assets segment for years, and that it intends to build a regulatory framework to ensure the solidity of market players, compatibility with the risks of the business models, and the sustainable development of innovations.[19]

The new regulations are expected to be enacted by the end of 2023, after BCB has held public consultations, and should establish the criteria to authorise VASP operation, define functional and conduct aspects, as well as adopt risk, capital management and fraud prevention guidelines. Other topics of attention under the Legal Framework for Virtual Assets shall be regulated, such as adopting the principles of free enterprise, free competition and consumer protection, as well as international recommendations and best practices.

In summary, BCB has high expectations on the development and launch of Real Digital and believes that its implementation will indeed significantly transform the Brazilian financial system. Roberto Campos Neto, BCB's Governor, stated in August 2022 that the entity intends to regulate the market to provide more transparency to investors and players, and pointed out that regulation should be focused on creating opportunities for innovation and new technologies, and not on preventing them.[20] The proper launch of Real Digital is expected to take place by the end of 2024.[21]

Cryptocurrency regulation

Introduction

Technological transformations brought about significant challenges to the Brazilian legal system. Over the last few years, a series of bills of law were proposed in the National Congress concerning digital assets – most of which aimed to address societal concerns and decrease systemic vulnerabilities regarding fraud and Ponzi schemes, while some introduced probate and succession rules for digital assets, as discussed in more detail below.

Legislative discussions and bills of law

House Bill of Law No. 4,401/21[22] (originally proposed as House Bill of Law No. 2,303/15[23] and further renumbered), presented on July 8, 2015, was the first initiative to regulate cryptoassets in Brazil, and was later approved and converted into the Legal Framework for Virtual Assets in 2022, after comprising and incorporating several other bills of law proposed over the following years that addressed similar or related subjects. Originally, House Bill of Law No. 2,303/15 was drafted and further discussed to address concerns with fraudulent schemes and to increase the prevention of money laundering. However, it relied on a questionable generalisation of cryptocurrencies as a sort of "*electronic currency*" and embraced, under the same rules, the loyalty programmes (such as air carriers' mileage bonuses). The intention was to enable prudential regulation by BCB, establish integration with the "*payment arrangements*" system set by Law No. 12,865/13, and facilitate further enforcement of anti-money laundering/combatting the financing of terrorism ("**AML/CFT**") rules.

Later, in 2019, House Bill of Law No. 2,060/19[24] was presented, bringing more complete and precise definitions regarding cryptographic values, instruments, assets, rights and services, and virtual tokens. It also introduced rules for the issuance of cryptoassets and defined their fraudulent use in "*pyramid*" or Ponzi schemes as a criminal offence, as well as in other irregular transactions. In parallel, several bills of law were presented at the Senate regarding virtual currency regulation more broadly, namely Bills of Law Nos 3,825/19,[25] 3,949/19,[26] and 4,207/20.[27] Besides working more consistently with definitions and classifications, they also focused on fighting money laundering and other illicit practices. These four bills of law were attached to House Bill of Law No. 2,303/15, which on its turn was renumbered in the Senate as 4,401/21. After passing a vote in the Senate, it was enacted as Law No. 14,478/22 – the Legal Framework for Virtual Assets – on December 21, 2022.

Legal Framework for Virtual Assets

As previously noted, the Legal Framework for Virtual Assets was enacted on December 21, 2022, and became effective as of June 20, 2023. It focused on more general concepts and principles regarding the provision of services by VASPs, while BCB was further designated the competent entity to enact the proper regulation of the sector, considering the guidelines and rules set forth in the law. The main provisions and guidelines of the Legal Framework for Virtual Assets can be summarised as follows:

(i) **Scope (Section 1)**: The law provides guidelines and rules to be observed in the "*provision of virtual assets services and in the regulation of virtual assets providers*", expressly stating that it is not applicable to virtual assets that represent securities, which are subject to the regulation and supervision of the Brazilian Securities and Exchange Commission (*Comissão de Valores Mobiliários* – "**CVM**"), the agency in charge of commodities and securities markets, while also noting that CVM's competence is not altered by it in any way (Section 1, Sole Paragraph).

(ii) **Definition of "virtual asset" (Section 3)**: "*Virtual asset*" is defined as "*the digital representation of value that can be traded or transferred by electronic means and used for payment or investment purposes*". A few items were expressly excluded from this definition: (a) national and foreign currencies; (b) electronic currencies, pursuant to Law No. 12,865/13; (c) instruments that provide the holder with access to specified products or services, such as points and rewards from loyalty programmes; and (d) representations of assets whose issuance, bookkeeping, trading or settlement is provided for by law or regulation. Notwithstanding the fact that the Legal Framework for Virtual Assets brought important outlines to the concept of "virtual asset" – clearly encompassing in this definition, for example, "cryptocurrencies" – it was widely criticised by the market for not expressly mentioning tokens and their various forms and functions. Until now, the main formal regulatory act to have addressed and confronted the issue of tokens in Brazil was CVM Guidance Opinion No. 40 (*Parecer de Orientação* CVM No. 40/2022),[28] published on October 11, 2022 by CVM, in which the entity expressed its understanding on which virtual assets would be considered securities and would therefore be subject to its regulation and supervision. This topic is detailed in "The definition and regulation of "tokens"" section below.

(iii) **Definition of "VASPs" (Section 5)**: VASPs are defined as legal entities that perform, on behalf of third parties, at least one of the following services: (a) exchange between virtual assets and national or foreign currency; (b) exchange between one or more virtual assets; (c) transfer of virtual assets; (d) custody or administration of virtual assets or instruments that allow control over virtual assets; or (e) participation in financial services and provision of services related to an issuer's offer or sale of virtual assets. According to Section 5, BCB may further authorise the performance of other services that are directly or indirectly related to such activities.

(iv) **Authorisation to operate (Section 2)**: VASPs may only operate in Brazil with prior authorisation from BCB. However, the specific rules and requirements to obtain authorisation have not yet been created and enacted and currently, in practice, it is not possible to request such authorisation to the entity. This regulatory gap has created a scenario of legal uncertainty regarding the situation of VASPs that intend to start their operations after the entry into force of the Legal Framework for Virtual Assets but before the publication of the rules to obtain such authorisation to operate by BCB. Despite this, it is reasonable to conclude that, for now, VASPs that intend to start their

operations do not need to request such authorisation – after all, this request is not possible for the time being, and such a prohibition would violate several principles of Law No. 13,874/19 ("**Brazilian Economic Freedom Law**"),[29] which establishes rules to protect free enterprise and the free exercise of economic activity.

(v) **Adequacy of VASPs already in operation (Section 9)**: The Legal Framework for Virtual Assets provided that BCB shall define the conditions and deadlines for VASPs already in operation to comply with the terms of the law and other related rules, on the condition that such period for compliance cannot be less than six months.

(vi) **BCB's competences and attributions (Section 7)**: According to the Legal Framework for Virtual Assets, BCB shall have, among others, the following attributions: (a) authorise both the operation of VASPs and certain of their corporate operations (such as transfers of control, mergers and incorporations); (b) establish conditions for the exercise of positions in statutory and contractual bodies within VASPs, and authorise the exercise of management positions by individuals; and (c) supervise VASPs in general and apply the provisions of Law No. 13,506/17, which concerns the rules of BCB's administrative sanctioning process, in case of non-compliance with the Legal Framework for Virtual Assets.

(vii) **Criminal aspects (Sections 10, 11 and 12)**: The Legal Framework for Virtual Assets provided for: (a) the amendment and inclusion, in the Brazilian Penal Code (Decree-Law No. 2,848/40),[30] of the crime of fraud specifically related to virtual assets, securities or financial assets, with a criminal penalty of four to eight years of imprisonment; (b) the equivalence of wallets and exchanges to financial institutions, with regard to the characterisation of crimes against the National Financial System (Law No. 7,492/86);[31] and (c) the increase in the penalty of the crime of money laundering from one-third to two-thirds, if carried out through the use of virtual assets (Section 1, Paragraph 4, Law No. 9,613/98).[32]

(viii) **Control and supervision by COAF (Section 10, II)**: The Legal Framework for Virtual Assets included VASPs in Section 9 of Law No. 9,613/98,[33] which lists the entities subject to the control and supervision mechanisms of the Council of Financial Activities Control (*Conselho de Controle de Atividades Financeiras* – "**COAF**"), a federal agency linked to BCB, responsible for regulating, supervising and applying administrative penalties in regard to certain financial crimes, such as money laundering and financing of terrorism. Despite that, the obligation of VASPs to maintain customer records and report information to COAF will only become effective with the actual enactment of the regulation by BCB, since Law No. 9,613/98 establishes that such obligations before COAF must observe the rules and guidelines issued by the competent authority, which have yet to be issued (Sections 10 and 11).

(ix) **Application of the Consumer Protection Code (Section 13)**: The Legal Framework for Virtual Assets stated that the provisions of the Consumer Protection Code (Law No. 8,078/90)[34] shall apply to operations conducted in the virtual assets market, whenever applicable.

(x) **Absence of a provision for separation of assets**: It is worth noting that, during the legislative discussion of House Bill of Law No. 4,401/21, the provisory text determined that VASPs should segregate their own financial resources, virtual assets and respective ballasts from those held for the account and order of third parties (former Section 13, Paragraph 1, of House Bill of Law No. 4,401/21). This topic was the subject of strong debate and was ultimately not approved in the final text. Nonetheless, it is possible that BCB will introduce this obligation under its regulatory mandate.

The definition and regulation of "tokens"

As discussed above, Section 3 of the Legal Framework for Virtual Assets defined "virtual asset" as a "*digital representation of value that can be traded or transferred electronically and used for payments or investment purposes*".[35] While the Legal Framework for Virtual Assets provided some guidelines for this definition, it has been criticised by the market for not explicitly mentioning tokens and their various forms and functions, leading to some legal uncertainty regarding their treatment.

On the one hand, pursuant to Section 3, a "digital asset" is defined as a "*digital representation of value*", without the explicit mention of digital representations of "rights" (which theoretically excludes certain assets from its definition, such as utility tokens). On the other hand, Section 3 states that "virtual assets" are those used "*for payments or investment purposes*". As such, this delimitation in regard to the purpose of the assets theoretically excludes various types of tokens that are not used specifically for payment or investment (such as utility tokens yet again).

Nonetheless, although they are not explicitly mentioned in the Legal Framework for Virtual Assets, there is a common understanding and recognition by the market and by various relevant governmental entities that tokens are considered virtual assets under this law. In this regard, RFB[36] and CVM, for example, have already expressed their views (as per CVM Guidance Opinion No. 40/22).

BCB, on the other hand, has not yet formally expressed its position in this regard. However, it is expected by the market that the entity will formally include the various forms of tokens (except those that represent securities) within its regulatory framework, as one of its prerogatives is "*establishing which financial assets will be regulated*" for the purposes of the Legal Framework for Virtual Assets (pursuant to Section 3, Sole Paragraph).

In summary, it is important to bear in mind that, for now, despite the legal uncertainty, there are strong arguments to support the notion that "tokens" are also considered "virtual assets" within the scope of services provided by VASPs, except when they bear characteristics that qualify them as "securities", in which case they would be subject to the regulation and supervision of CVM.

CVM Guidance Opinion No. 40/2022 – classification of tokens

Although it does not have force of law and was published shortly before the Legal Framework for Virtual Assets, CVM Guidance Opinion No. 40/22 is one of the main references for the definition and classification of tokens and shall most likely be taken into consideration by BCB in the forthcoming regulation.

According to CVM Guidance Opinion No. 40/22, CVM adopted a functional approach to differentiate the various types of tokens, and the classification indicates the appropriate legal treatment for each token type. Initially, the following categories were listed by the entity:

(i) **Payment token (cryptocurrency or payment token)**: A token that seeks to replicate the functions of currency, notably as a unit of account, means of exchange, and store of value.
(ii) **Utility token**: A token used to acquire or access certain products or services.
(iii) **Asset-backed token**: A token that represents one or more tangible or intangible assets. Examples include security tokens, stablecoins, non-fungible tokens ("**NFTs**"), and other assets subject to tokenisation operations.

CVM clarified that the aforementioned categories are not exclusive or rigid, so a single cryptoasset may fall into one or more categories, depending on the functions it performs and its associated rights. Additionally, the proposed division is meant to be merely initial and may be changed or expanded by the entity whenever necessary, in line with industry developments.

In summary, according to CVM, an asset-backed token may or may not be considered a security. This determination depends on the verification, in the specific case, of the economic essence of the rights conferred to its holders. According to the entity, a cryptoasset will be considered a security when it:

(i) is a **digital representation of a security**, such as shares, debentures, certificates of receivables, and derivatives, regardless of the nature of the underlying assets; or

(ii) falls within the definition of **collective investment contract**, which is a security or contract that, when publicly offered, generates participation, partnership, or remuneration rights, including those resulting from service provision (as per the broad definition of collective investment contract provided for in Section 2, IX, of Law No. 6,385/76).[37]

The Brazilian legal concept of collective investment contract is strongly inspired by US law, especially the precedent of the Supreme Court of the United States that resulted in the so-called "*Howey* Test", which determines the criteria for an asset to be considered a security.

In any case, it is important to note that if considered a security, not only does the virtual asset itself become subject to CVM regulation, but also the service provider related to it. Finally, it is worth noting that the intermediation of buying and selling securities for third parties is an activity permitted only to institutions duly authorised by CVM, subject to its regulation and supervision, as provided in Section 3 of CVM Resolution No. 35/21.[38]

Other relevant bills of law

In addition to the Legal Framework for Virtual Assets, there are other bills currently under discussion by the National Congress, which address specific points related to cryptoassets.

In the House of Representatives, for instance, there are some projects that intend to amend the Civil Procedure Code (Law No. 13,105/15),[39] including provisions and procedures related to cryptocurrencies within the scope of law suits (House Bills of Law Nos 743/22,[40] 1600/22,[41] and 462/22).[42] In its turn, House Bill of Law No. 3,908/21[43] establishes that employees from the private and public sector may receive part of their compensation in cryptocurrencies, if so agreed by the parties. Additionally, House Bill of Law No. 462/22[44] provides for the crime of embezzlement specifically related to cryptoassets.

In the Senate, there are also bills discussing various themes related to cryptoassets. For instance: (i) Senate Bill of Law No. 3,706/21,[45] which concerns the fraudulent "pyramid" or Ponzi schemes and irregular transactions with cryptoassets; and (ii) Senate Bill of Law No. 3,876/21,[46] which concerns the civil liability of cryptoasset exchanges, specifically in relation to duties towards clients and account handling.

Sales regulation

Introduction

Discussions regarding the interaction of cryptoassets and capital markets regulation have been held since at least 2017, when CVM introduced its equity crowdfunding rules by issuing CVM Instruction No. 588/17, further revoked and replaced by CVM Resolution No. 88/22 in April 2022.[47]

In October 2017, CVM released a statement on Initial Coin Offerings ("**ICOs**"), and noted that "*ICOs can be understood as a form of raising funds from the investing public, the counterpart being the issuance of virtual assets (tokens or coins), which, depending on the economic context of issuance and on the rights conferred to investors, may meet the definition of securities*".[48] The agency issued CVM/SRE Letter No. 02/2019[49] in February 2019 to restate its conclusions that certain virtual assets would be considered securities only if certain

rights were granted to the acquirer of the coin or token, such as capital equity, participation in agreements of pre-fixed compensation over the invested capital, or voting rights in meetings that define the direction of the issuer's business. Overall, as noted, CVM has been applying the fundaments of the *Howey* Test to assess the proper legal classification of these assets.

In October 2019, CVM brought its first enforcement investigation.[50] Promoters of a cryptocurrency were accused of conducting an unregistered ICO, and the Commission found that several provisions of securities regulations were violated. In October 2020, CVM commissioners unanimously agreed with the rapporteur's function-over-form analysis, according to which the classic definition of security was met. In their opinion, the offer was aimed to promote the investment in a collective scheme where profits were expected to arise largely from the efforts of offerors or third parties. The final order imposed on the promoters a disgorgement fine in excess of BRL 775,000.[51] Recently, on February 7 and 8, 2023, the Council of Appeals of the National Financial System (*Conselho de Recursos do Sistema Financeiro Nacional*) judged the administrative appeal against the promoters unanimously, considering that there was an irregular ICO without proper registration at CVM.[52]

In January 2020, CVM was faced with its first case involving a utility ICO. After a preliminary assessment by its analysts, CVM commissioners decided that the offer was not subject to CVM jurisdiction, as it involved utility tokens. Such tokens were not deemed securities given that the potential purchasers would not be granted gain, profit, or participation rights, but only the purchase of an asset with a specific utility or function.[53] While stressing that not all ICOs are public offers of securities, CVM pointed out that non-compliant offers would be considered illicit and, as such, subject to applicable sanctions and penalties under the securities law framework.

CVM has also adopted very strict scrutiny regarding virtual asset trading, especially with respect to foreign trading platforms targeting and offering their services to Brazilian clients while not licensed with the securities regulator. Several stop orders have been issued to those platforms, as well as to Brazilian unregistered companies offering investment schemes involving cryptocurrencies.[54] In several cases, Ponzi schemes have been identified, leading to a number of criminal indictments by public prosecutors. Nevertheless, innovative products and services developed with blockchain technologies can lead to assets that are not necessarily securities and, as such, would not fall within the scope of CVM oversight according to the entity itself, as detailed in the "Promotion and testing" section below.

Outlook

In view of the appointment of BCB as the competent entity to regulate, authorise and supervise the activity of VASPs, CVM issued a public statement on June 14, 2023[55] to reinforce that the Legal Framework for Virtual Assets does not interfere in the entity's competence and does not apply to activities involving securities that are digitally represented in the form of tokens.

According to CVM's public statement, tokens that are considered securities must adhere to the entity's regulations, particularly when it comes to raising funds from investors through public offerings of distribution.

It is worth noting that, through its own regulatory sandbox initiative,[56] CVM has approved three projects involving the issuance and trading of digitally represented securities tokens. In addition, CVM's regulatory agenda for 2023 includes projects that aim to develop a new regulatory framework for the establishment and management of organised securities markets, including token-based securities, in view of the experiences gained from CVM's regulatory sandbox. According to the entity, the goal of this project is to create regulations that are compatible with the transaction volumes and the complexity of such emerging markets.

Taxation

Given that cryptocurrencies represent valuable property rights, taxation follows general applicable rules to movable goods. Holders must declare their virtual assets in income tax statements, which are subject to capital gains arising from sales. In cases where gains are limited to BRL 35,000 per month, no taxation would be levied. Otherwise, they are taxed for capital gains in rates that may vary from 15% (gains under BRL 5 million) and 22.5% (gains over BRL 30 million).

RFB stated, through Query Solution (*Solução de Consulta*) No. 214/21,[57] that the exchange of cryptocurrencies without their conversion, at any time, into legal tender (BRL), is also subject to taxation over capital gain. In response, in February 2022, Bill of Legislative Decree (*Projeto de Decreto Legislativo*) No. 3/22[58] was proposed in the House of Representatives in order to suspend the effects of such Query Solution, on the grounds that taxation of the exchange, in these terms, would violate income tax legislation. The bill currently awaits a vote in the House of Representatives, and, if approved, will go to Senate for review and further voting.

In its turn, in April 2022, the Chamber of Foreign Trade (*Câmara de Comércio Exterior*), an entity linked to the Ministry of Economy, enacted Resolution No. 332/22[59] (further amended by Resolution No. 339/22)[60] to reduce to zero the import duty (*Imposto de Importação*) levied on cryptocurrency mining equipment that utilises the SHA256 algorithm and on cryptocurrency hardware wallets. Resolution No. 332/22 defines these wallets as "*cryptocurrency storage devices, supporting Bitcoin, Ethereum, XRP, Bitcoin Cash, EOS, Stellar, among other digital currencies, secure bitcoin wallet, with the function of connecting any computer via USD and with built-in OLED screen for double checking and confirmation of transactions with a single touch of its buttons*". The reduction of import duty is temporary, and will be in force until December 31, 2025.

Finally, as discussed below, estate or inheritance taxes on goods, assets or other rights are levied between 2% and 8%, according to the state in which the deceased was resident.

Money transmission laws and anti-money laundering requirements

Brazilian authorities have already expressed concerns with the use of cryptocurrencies for money laundering purposes, and, as discussed above, several bills of law were presented in the National Congress to include preventive reporting obligations.

The Legal Framework for Virtual Assets, in its turn, established that VASPs must generally comply with the following guidelines regarding the matter: (i) adoption of good governance practices, transparency in operations and a risk-based approach (Section 4, II); and (ii) controls on AML/CFT and on the proliferation of weapons of mass destruction, in line with international standards (Section 4, VII).

The Legal Framework for Virtual Assets did not specify how such guidelines should be observed, leaving such detailing, as mentioned, to BCB's forthcoming regulation. Nonetheless, Section 12 included VASPs among the list of entities subject to certain control and supervision mechanisms of COAF – they are required to identify clients, keep records of activities and report certain transactions, pursuant to Sections 10 and 11 of Law No. 9,613/98.[61] Despite that, such obligations will only become properly effective when BCB enacts its regulation, as mentioned in the "Legal Framework for Virtual Assets" section above.

In summary, COAF is a federal agency – now a department of BCB – that is at the centre of financial intelligence and in charge of suspected cases of concealment of assets and values, money laundering and financing of terrorism. COAF's legal mandate includes coordination

with sector-specific supervisory agencies and regulatory and enforcement powers for industries that are not subject to oversight by government bodies.

A series of economic players must report transactions carried out to COAF in matters that may trigger money laundering risks. While banking, capital market, insurance, and pension fund players are the most common entities subject to its supervisory activities, professional athlete agency companies, accounting firms, jewellery and precious metals, factoring, lotteries, and art dealing companies must also report suspicious transactions to COAF. Reports usually include know-your-client and internal compliance measures, identification and recordkeeping of customers and deals, as well as disclosure of transactions in excess of certain amounts. The reporting procedures were restated in March 2021 by COAF Resolution No. 36/21.[62] Covered entities must periodically run internal risk assessments according to the amounts and volumes of their operations, and once an entity is notified by COAF of a suspected transaction, it must submit an online form (Electronic Compliance Assessment) aimed at improving its internal controls.[63]

In addition to authority-mandated information requirements, rules expedited by self-regulatory industry bodies have been adopted in order to assist in AML/CFT activities. For example, exchanges have been vastly accepting the rules set by the Brazilian Association of Cryptoeconomy (*Associação Brasileira de Criptoeconomia* – "**ABCripto**"), which requires firms involved in crypto exchange and brokerage to introduce additional measures in their platforms to avoid transactions that might characterise illicit activities or financial crimes.[64] Until recently, although this practice was not mandatory, many VASPs, following ABCripto's guidelines, informed COAF about suspicious cryptocurrency transactions through a specialised channel in the entity's system, i.e., Siscoaf.

In late August 2022, however, COAF announced that it would discontinue VASPs' access to Siscoaf, as such access would only be provisional and experimental, as part of the preparation and evaluation of the entity for the new reality of virtual asset transactions. According to COAF, this evaluation period has been concluded, and such access was to be suspended at least until the approval of the former House Bill of Law No. 4,401/21, the Legal Framework for Virtual Assets, which expressly included VASPs in the list of institutions required to provide information to the body. Despite market criticism at the time, in September 2022, COAF released a public note informing that, until the Legal Framework for Virtual Assets was approved, any suspicious activities could still be reported to the agency, regardless of access to Siscoaf, including through the "Fala.Br" platform, an official government platform to report suspicious or illegal activity.[65] Nonetheless, at the time of writing, in July 2023, after the enactment of the Legal Framework for Virtual Assets, no official or specific channels have yet been provided by COAF for VASPs to fulfil their obligations.

In turn, recent BCB administrative regulations have been enacted to reinforce AML/CFT measures. While not specifically concerning crypto exchanges, the new rules are generally followed by firms as they usually have plans to become financial institutions regulated by BCB. Additionally, the purported fragility of AML/CFT safekeeping measures has been the main argument used by banks to close exchange accounts. In this respect, in January 2020, BCB Circular No. 3,978/20 imposed policies, procedures, and internal controls to be adopted by regulated entities to prevent the use of the financial system for such illegal activities.[66] It was followed by BCB Circular Letter No. 4,001/20, which presented a non-exhaustive list of events that point out potential crimes of money laundering or concealment of assets, rights and values and financing of terrorism, subject to the imposed monitoring procedures. BCB Circular No. 3,978/20 was amended in July 2021 and again in December 2022 to include additional measures and mandatory information to be followed by financial institutions.

Promotion and testing

In September 2019, the Brazilian Economic Freedom Law established a Declaration of Economic Freedom Rights. It purports to simplify general governmental requirements, reduce bureaucracy for economic players, as well as promote cultural changes in interactions among private businesses and Brazilian authorities. It sets forth provisions to assure minimum state intervention and reduction of government control of the markets, and to further expand initiatives such as regulatory sandboxes to foster competition and innovation in the Brazilian economy.

As a direct reflex of the Brazilian Economic Freedom Law, three main agencies under the Ministry of Economy, BCB, CVM, and the Superintendence of Private Insurances (*Superintendência de Seguros Privados* – "**SUSEP**", which is responsible for the supervision and control of the insurance market and private pension funds), announced that they had agreed to introduce sandbox programmes to implement emerging technologies under more relaxed regulatory provisions. The agencies also announced that they would integrate blockchain applications into their own workflows.[67]

Thereby, in October 2020, the National Monetary Council (*Conselho Monetário Internacional* – "**CMN**"), which is the major institution of the Brazilian financial system and supervises the activities of other regulatory and enforcement agencies, enacted CMN Resolution No. 4,865/20,[68] which frames regulatory sandboxes in the financial sectors regulated by BCB, CVM and SUSEP.

BCB's sandbox principles were then set by BCB Resolution No. 29/2020,[69] complemented by BCB Resolution No. 50/2020,[70] which defined the core regulation for the establishment, execution, and related procedures for the first batch of companies engaged in financial and payment innovations. Unlike LIFT, mentioned above, BCB's sandbox aims to follow and develop innovative projects that are already mature, but in which there is a need to validate the business model through its effective implementation. In addition, it enables participants to provide products and services to real customers. Of the 52 projects then submitted, seven were selected in November 2021 and are participating in the development cycle, which may be extended until the end of 2023.

Among the projects approved and under development, a few examples can be mentioned: (i) a solution that allows the execution of payment transactions with credit concession, revolving or in instalments, using features of the Brazilian instant payment method PIX; (ii) a platform for the issuance and secondary trading of fixed-income securities; and (iii) the development of a secondary market for Bank Credit Notes. At the end of the cycle, the participants will have the chance to obtain the definitive authorisation to operate, and the projects developed can serve as a basis to improve BCB and CMN regulations.[71] On December 16, 2022, BCB published a formal report on the projects' current progress and further expectations.[72]

SUSEP's sandbox framework, which focuses on the establishment of an open insurance environment, was adopted in March 2020 by Resolution No. 381/20,[73] amended by Resolution No. 417/21 in July 2021.[74] The first batch of the initiative was launched in 2020, in which 11 projects took part, devoted to enhancing innovation in insurance products and services. The second batch of SUSEP's sandbox programme was launched in late July 2021 and selected 21 projects, covering innovative solutions for different market demands and sectors.[75] Among them, the initiatives range from pay-per-use insurance and intermittent coverage for car, residential and sports protection, to damage microinsurance, truck insurance, insurance for passengers who seek to reduce losses with cancellation and

rebooking of airline tickets and hotels, and parametric agricultural insurance with the use of advanced technologies for monitoring and regulating claims, focused on the inclusion of small and medium-sized rural producers.

Lastly, CVM's sandbox rules adopting its own regulatory safe harbour were established in May 2020 by CVM Instruction No. 626/20,[76] replaced in May 2021 by CVM Resolution No. 29/21.[77] Its goals include to foster innovation in capital markets, enhance competition and provide greater inclusion as a result of new financial services. In July 2021, CVM made public the preliminary list of proponent companies for its first batch of sandbox projects, including an overview of the main challenges addressed by applicants. Of the 33 projects originally submitted, four were approved (three in September 2021[78] and an additional one in December 2021)[79] and granted temporary authorisation to operate.

In summary, the four projects approved in CVM's sandbox concern the following companies and activities: (i) a securities bookkeeper that will provide services to limited liability companies that have carried out or are in the process of carrying out public offerings of securities via crowdfunding, as regulated in CVM Resolution No. 88/22;[80] (ii) two platforms that provide the issuance, public distribution, and trading of securities issued or represented in the form of tokens based on blockchain networks, both on an organised over-the-counter market and in the context of equity crowdfunding, under the framework of CVM Resolution No. 88/22;[81] and (iii) a platform that provides the issuance and trading of tokens of debentures and shares of closed-end investment funds, specifically targeted at qualified investors (with at least BRL 1 million in investments), under the framework of CVM Instruction No. 476/09.[82]

Recently, in March 2023, CVM authorised one of the sandbox's participating companies to start the issuance, public distribution and trading, in the over-the-counter market, of tokens of startups that raised funds through crowdfunding.[83] The operation of the company is already active in Brazil.[84]

Ownership and licensing requirements

CVM does not currently allow investment funds to directly purchase or invest in cryptocurrencies. These funds are regulated by CVM Instruction No. 555/2014[85] and, according to CVM/SIN Circular Letter No. 01/18, issued in January 2018,[86] these virtual assets may not always be qualified as financial assets. The capital markets agency also indicated that fund managers should perform proper due diligence to analyse the correct risk of this form of investment, and that there are numerous risks such as fraud, decreased liquidity, hacking security incidents, and financing of illegal activities, among others.

On the other hand, CVM/SIN Circular Letter No. 11/18 expressly allowed indirect investments in cryptocurrencies.[87] In March 2021, CVM approved Exchange-Traded Funds ("**ETFs**") based on indirect cryptoasset investments. In late April 2021, the first Brazilian Bitcoin-based ETF was launched in the São Paulo Stock Exchange, replicating the Nasdaq Crypto Index.[88] It was followed in July 2021 by the first Ethereum-based ETF, providing investors with safe custody and daily liquidity, without them having to worry about private keys.[89] Since then, the market has grown significantly. Nowadays, there are several ETFs and investment funds focused on cryptoassets registered and available at the São Paulo Stock Exchange.

Mining

Mining activity is permitted and has not been regulated by any entity. However, according to RFB, economic gain from the sale of tokens must be taxed as capital gains. Even if

the tokens issued are not sold, both individuals and companies must report the amount of cryptocurrency they own, even if they result from mining activities. Upon recommendation of the International Monetary Fund,[90] since August 2019, BCB has been classifying cryptocurrency mining activity as a productive process, and therefore considers that non-financial assets are produced, i.e., assets that have come into existence as outputs from production processes within the borders of a country.[91]

In addition, as described in the "Taxation" section above, the import tax rate on mining equipment using the SHA256 algorithm has been temporarily reduced to zero until December 31, 2025.

Border restrictions and declaration

BCB stated in one of its *communiqués* that transactions with virtual currencies and other instruments that require international transfers are subject to foreign exchange regulations, in particular the carrying out of transactions exclusively through institutions authorised by BCB to operate in the exchange market.

As for the Travel Rule, although Brazil is a member of the Financial Action Task Force ("**FATF**"), this topic has not yet been addressed in any relevant instance.

Reporting requirements

At least since 2016, RFB has been publishing specific instructions on how individuals should report their virtual asset holdings for income tax purposes on their tax returns. RFB Normative Ruling No. 1,888/19 requires cryptoasset exchanges to disclose specific transaction data from its clients, including information such as the parties involved in the negotiation of assets, related dates, addresses of the remittance and receiving wallets, and amounts and fees involved. Parties engaging in sales must also file disclosure information if monthly amounts are in excess of BRL 30,000. Failure to notify such transactions may trigger penalties ranging between BRL 1,500 and 3% of the amounts involved in the transactions for each unreported event.

Cryptoassets must also be declared by individuals to RFB in their annual income tax return, specifically in the "Assets and Rights" sheet, whenever the acquisition amount of each type of cryptoasset is equal to or in excess of BRL 5,000. RFB's electronic return system provides for specific codes according to asset type as follows: (i) Bitcoin; (ii) other cryptocurrencies, such as altcoins; (iii) stablecoins; (iv) NFTs; and (v) other cryptoassets not included above.[92]

Estate planning and testamentary succession

Given that cryptoassets are considered goods or movable property, general probate and succession rules apply, including for estate or inheritance taxes (which are levied between 2% and 8% according to the state in which the deceased was resident). Court decisions discussing specifics of digital estates are scarce, and no precedents have been found with regard to virtual assets.

In a recent ruling, the São Paulo State Court of Appeals (*Tribunal de Justiça do Estado de São Paulo*) declared that successors had no standing to request access to the deceased's Facebook account.[93] The user had not agreed to the terms and conditions provision to permit access to third parties in case of death. The panel of appeal judges declared the account a strictly personal service with no economic probate effects, and decided it should be deleted.

Probate law practitioners have increasingly been advising clients to create digital estate plans by taking inventory of digital assets and cryptoassets, especially to provide access to passwords and access phrases to digital wallets and similar devices or schemes. As will deeds are publicly accessible in Brazil, a codicil or similar private document would be the best arrangement to avoid pitfalls for beneficiaries.

As a result of the increasing dilemmas regarding transmission of digital estates, legislators have been discussing the matter, which resulted in Senate Bill of Law No. 6,468/19[94] and House Bill of Law No. 3,050/20.[95] Both pieces of proposed legislation specifically permit a decedent's executor to access and manage digital assets and convey them to the beneficiaries.

* * *

Endnotes

1. https://www.planalto.gov.br/ccivil_03/_ato2019-2022/2022/lei/L14478.htm
2. https://www.planalto.gov.br/ccivil_03/_Ato2023-2026/2023/Decreto/D11563.htm
3. https://www.bcb.gov.br/detalhenoticia/705/noticia
4. https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2013/lei/l12865.htm
5. https://www.bcb.gov.br/pom/spb/ing/Communique_25306.pdf
6. https://www.bcb.gov.br/pom/spb/ing/Communique_31379.pdf
7. https://www.bcb.gov.br/estabilidadefinanceira/lift
8. A comprehensive list of developed projects can be found at https://revista.liftlab.com.br/lift/issue/view/19/30
9. https://www.bcb.gov.br/site/liftchallenge/en
10. https://www.bcb.gov.br/detalhenoticia/672/noticia
11. https://www.in.gov.br/en/web/dou/-/portaria-n-108.092-de-20-de-agosto-de-2020-273476769
12. https://www.bcb.gov.br/en/pressdetail/2397/nota
13. https://www.bcb.gov.br/detalhenoticia/593/noticia
14. https://www.bcb.gov.br/site/liftchallenge/en
15. https://www.bcb.gov.br/detalhenoticia/667/noticia
16. https://github.com/bacen/pilotord-kit-onboarding
17. https://exame.com/future-of-money/banco-central-confirma-real-digital-funcao-congelar-valores
18. https://portal.tcu.gov.br/levantamento-da-tecnologia-blockchain.htm
19. https://www.bcb.gov.br/detalhenoticia/17919/nota
20. https://www.infomoney.com.br/mercados/campos-neto-defende-modelo-do-real-digital-e-regulacao-que-nao-atrapalhe-inovacao
21. https://www.infomoney.com.br/minhas-financas/real-digital-podera-ser-testado-com-a-populacao-no-fim-de-2024-se-piloto-tiver-sucesso-diz-bc
22. https://www25.senado.leg.br/web/atividade/materias/-/materia/151264
23. https://www.camara.leg.br/proposicoesWeb/fichadetramitacao?idProposicao=1555470
24. https://www.camara.leg.br/proposicoesWeb/fichadetramitacao?idProposicao=2196875
25. https://www25.senado.leg.br/web/atividade/materias/-/materia/137512
26. https://www25.senado.leg.br/web/atividade/materias/-/materia/137644
27. https://www25.senado.leg.br/web/atividade/materias/-/materia/144036
28. https://conteudo.cvm.gov.br/legislacao/pareceres-orientacao/pare040.html
29. https://www.planalto.gov.br/ccivil_03/_Ato2019-2022/2019/Lei/L13874.htm

30. https://www.planalto.gov.br/ccivil_03/decreto-lei/del2848compilado.htm
31. https://www.planalto.gov.br/ccivil_03/leis/l7492.htm
32. https://www.planalto.gov.br/ccivil_03/leis/l9613compilado.htm
33. https://www.mpf.mp.br/atuacao-tematica/sci/normas-e-legislacao/legislacao/legislacao-em-ingles/law-9-613-anti-money-laundering-law/view
34. https://www.planalto.gov.br/ccivil_03/leis/L8078compilado.htm
35. A definition close to that proposed by the Financial Action Task Force, as available at https://www.fatf-gafi.org/en/topics/virtual-assets.html#:~:text=Virtual%20assets%20(crypto%20assets)%20refer,many%20potential%20benefits%20and%20dangers
36. As understanding provided for in Normative Ruling No. 1,888/19.
37. https://www.planalto.gov.br/ccivil_03/leis/l6385.htm
38. https://conteudo.cvm.gov.br/legislacao/resolucoes/resol035.html
39. https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2015/lei/l13105.htm
40. https://www.camara.leg.br/propostas-legislativas/2318856
41. https://www.camara.leg.br/propostas-legislativas/2327147
42. https://www.camara.leg.br/proposicoesWeb/fichadetramitacao?idProposicao=2317334
43. https://www.camara.leg.br/propostas-legislativas/2305840
44. https://www.camara.leg.br/proposicoesWeb/fichadetramitacao?idProposicao=2317334
45. https://www25.senado.leg.br/web/atividade/materias/-/materia/150410
46. https://www25.senado.leg.br/web/atividade/materias/-/materia/150600
47. https://conteudo.cvm.gov.br/legislacao/resolucoes/resol088.html
48. https://www.gov.br/cvm/pt-br/assuntos/noticias/initial-coin-offerings--icos--88b47653f11b4a78a276877f6d877c04
49. https://conteudo.cvm.gov.br/legislacao/oficios-circulares/sre/oc-sre-0219.html
50. https://conteudo.cvm.gov.br/export/sites/cvm/noticias/anexos/2020/20201026_PAS_CVM_SEI__19957_003406_2019_91_relatorio_diretor_gustavo_gonzalez.pdf
51. https://conteudo.cvm.gov.br/export/sites/cvm/sancionadores/sancionador/anexos/2020/SEI_19957003406_2019_91.pdf
52. https://www.gov.br/economia/pt-br/orgaos/orgaos-colegiados/conselho-de-recursos-do-sistema-financeiro-nacional/acesso-a-informacao/noticias/2023/crsfn-julga-primeiro-caso-de-processo-sancionador-da-cvm-envolvendo-criptoativos
53. https://conteudo.cvm.gov.br/decisoes/2018/20180130_R1/20180130_D0888.html
54. A comprehensive list of stop orders can be found at https://www.gov.br/cvm/pt-br/assuntos/protecao/alertas/deliberacoes-cvm-alertas-de-suspensao
55. https://www.gov.br/cvm/pt-br/assuntos/noticias/publicado-decreto-sobre-ativos-virtuais
56. https://conteudo.cvm.gov.br/legislacao/sandbox_regulatorio.html
57. https://normas.receita.fazenda.gov.br/sijut2consulta/link.action?idAto=122341
58. https://www.camara.leg.br/propostas-legislativas/2313803
59. https://www.in.gov.br/en/web/dou/-/resolucao-gecex-n-332-de-4-de-maio-de-2022-397587255
60. https://www.in.gov.br/en/web/dou/-/resolucao-gecex-n-339-de-9-de-maio-de-2022-398654148
61. https://www.mpf.mp.br/atuacao-tematica/sci/normas-e-legislacao/legislacao/legislacao-em-ingles/law-9-613-anti-money-laundering-law/view
62. https://www.gov.br/coaf/pt-br/acesso-a-informacao/Institucional/a-atividade-de-supervisao/regulacao/supervisao/normas-1/resolucao-coaf-no-36-de-10-de-marco-de-2021

63. https://www.gov.br/coaf/pt-br/centrais-de-conteudo/publicacoes/guia-de-preenchimento-da-avec_2022.pdf/view
64. ABCripto's Code of Conduct and Self-Regulation and Manual of Good Practices to Prevent Money Laundering and Financing of Terrorism are available at https://abcripto.com.br/autorregulacao
65. https://www.gov.br/coaf/pt-br/assuntos/noticias/ultimas-noticias/sobre-a-descontinuacao-de-acessos-experimentais-ao-sistema-de-controle-de-atividades-financeiras-siscoaf-na-condicao-de-empresa-prestadora-de-servicos-de-ativos-virtuais-psav
66. https://www.bcb.gov.br/estabilidadefinanceira/exibenormativo?tipo=Circular&numero=3978
67. https://www.bcb.gov.br/detalhenoticia/16776/nota
68. https://www.bcb.gov.br/content/config/Documents/Regulatory_Sandbox_Regulation_CMN_Resolution_No_4865_2020.pdf
69. https://www.bcb.gov.br/estabilidadefinanceira/exibenormativo?tipo=Resolu%C3%A7%C3%A3o%20BCB&numero=29
70. https://www.bcb.gov.br/estabilidadefinanceira/exibenormativo?tipo=Resolu%C3%A7%C3%A3o%20BCB&numero=50
71. https://www.bcb.gov.br/estabilidadefinanceira/sandbox
72. https://www.bcb.gov.br/detalhenoticia/647/noticia
73. https://www.in.gov.br/en/web/dou/-/resolucao-n-381-de-4-de-marco-de-2020-246507718
74. https://www.in.gov.br/en/web/dou/-/resolucao-cnsp-n-417-de-20-de-julho-de-2021-333273127
75. https://www.gov.br/susep/pt-br/assuntos/sandbox-regulatorio/sandbox-regulatorio-2a-edicao
76. https://conteudo.cvm.gov.br/legislacao/instrucoes/inst626.html
77. https://conteudo.cvm.gov.br/legislacao/resolucoes/resol029.html
78. https://www.gov.br/cvm/pt-br/assuntos/noticias/cvm-finaliza-primeiro-processo-de-admissao-do-sandbox-regulatorio
79. https://www.gov.br/cvm/pt-br/assuntos/noticias/cvm-aprova-mais-uma-proposta-para-o-sandbox-regulatorio
80. https://conteudo.cvm.gov.br/legislacao/deliberacoes/deli0800/deli873.html
81. CVM Deliberation No. 874 (https://conteudo.cvm.gov.br/legislacao/deliberacoes/deli0800/deli874.html) and CVM Deliberation No. 877 (https://conteudo.cvm.gov.br/legislacao/deliberacoes/deli0800/deli877.html).
82. https://conteudo.cvm.gov.br/legislacao/deliberacoes/deli0800/deli875.html
83. https://valor.globo.com/financas/criptomoedas/noticia/2023/03/29/cvm-autoriza-plataforma-smu-a-iniciar-negociao-tokens-de-startups-no-mercado-secundrio.ghtml
84. https://valor.globo.com/financas/criptomoedas/noticia/2023/07/13/smu-capta-r-1-milho-com-token-de-nota-comercial-de-startup-imobiliria.ghtml
85. https://conteudo.cvm.gov.br/legislacao/instrucoes/inst555.html
86. https://conteudo.cvm.gov.br/legislacao/oficios-circulares/sre/OC_SRE_0118.html
87. https://conteudo.cvm.gov.br/legislacao/oficios-circulares/sin/oc-sin-1118.html
88. https://www.b3.com.br/pt_br/noticias/b3-inicia-negociacao-do-primeiro-etf-da-hashdex.htm
89. https://www.nasdaq.com/articles/ethereum-etf-to-list-on-brazils-stock-exchange-2021-07-14
90. https://www.imf.org/external/pubs/ft/bop/2019/pdf/Clarification0422.pdf

91. https://www.bcb.gov.br/content/statistics/externalsectorstatistics_prev/201908_External_sector_statistics_text.pdf
92. https://www.gov.br/receitafederal/pt-br/centrais-de-conteudo/publicacoes/perguntas-e-respostas/dirpf/pr-irpf-2023/view
93. Appeal No. 1119688-66.2019.8.26.0100, decided on March 30, 2021 and still under discussion by the Superior Court of Justice (*Superior Tribunal de Justiça*) at the time of writing. Further information is available at https://www.tjsp.jus.br/Noticias/Noticia?codigoNoticia=63570
94. https://www25.senado.leg.br/web/atividade/materias/-/materia/140239
95. https://www.camara.leg.br/propostas-legislativas/2254247

Luiz Felipe Maia
Tel: +55 11 2175 5025 / Email: maia@mylaw.com.br

Luiz Felipe Maia is a founding partner at Maia Yoshiyasu Advogados and is the head of the technology and gaming area. He mainly counsels clients in corporate, contract and regulatory matters, including mergers and acquisitions, joint ventures, internet law, gaming law and strategic negotiations in related fields. He has worked as legal counsel for energy and IT companies, and has practised as an attorney in renowned law firms. He has a J.D. degree from the University of São Paulo, specialising in Business Law with a focus on contracts from Fundação Getúlio Vargas, and a Master's degree in Law from the Federal University of Pernambuco. He is also an experienced negotiator and mediator, certified by the Program on Negotiation at Harvard Law School, and teaches negotiation courses in business schools. He is a member of the International Association of Gaming Advisors, a general member of International Masters of Gaming Law, and the peer reviewer for Gambling Compliance in Brazil. He is a frequent speaker at international gaming events and, among other accolades, was recognised as Lawyer of the Year in Brazil for Gaming in 2019, 2020 and 2021 by *Corporate INTL* and *Global Law Experts*.

Flavio Augusto Picchi
Tel: +55 11 2175 5025 / Email: flavio@mylaw.com.br

Flavio Augusto Picchi is a partner at Maia Yoshiyasu Advogados in the technology and gaming area and an experienced attorney who works in connection with domestic and cross-border transactions and legal matters in a broad range of industries. Focused primarily on venture capital and capital markets, Flavio has worked in Brazil and in the United States, both in-house and in law firms. A pioneer in providing legal services to startup companies in Brazil, he holds an LL.M. degree in US and International Law from the University of Miami, and an M.Sc. degree in International Law from the University of São Paulo, where he also earned his LL.B. degree. He is a member of the Securities Law Committee of the Federal Council of the Brazilian Bar Association (OAB) and of the Business Law Section of the American Bar Association (ABA).

André Napoli
Tel: +55 11 2175 5025 / Email: anapoli@mylaw.com.br

André Napoli is an associate of the technology and gaming area at Maia Yoshiyasu Advogados, where he specialises in fintech, financial services regulation and startups. He holds an LL.B. degree from the Pontifical Catholic University of São Paulo (PUC-SP), an LL.M. degree in Tax Law from the Brazilian Institute of Tax Studies (IBET), and postgraduate degrees in Corporate Taxation and Fintechs and Payments from Fundação Getúlio Vargas (FGV-SP). He joined Maia Yoshiyasu Advogados in 2022 after working for several years as legal counsel for startups, fintechs and technology companies in Brazil.

Maia Yoshiyasu Advogados

Alameda Santos 2326, 1st floor, Sao Paulo, SP, Postal Code 01418-200, Brazil
Tel: +55 11 2175 5025 / URL: www.mylaw.com.br

British Virgin Islands

Chris Duncan & Katrina Lindsay
Carey Olsen

Government attitude and definition

The British Virgin Islands ("**BVI**") has established itself as a leading offshore finance centre that is resilient, agile and innovative in the face of regulatory changes, economic challenges and natural disasters. Companies, institutions and individuals, including those operating in the cryptocurrency, blockchain technology and Web3 space, use BVI vehicles to support their international business activities in order to benefit from the familiarity and stability of the BVI's English common law-based legal system, tax-neutral treatment and business-friendly flexibility of the BVI's regulatory and judicial regime.

The Government of the BVI works closely with the Island's industry leaders, from lawyers and accountants to insolvency practitioners and regulators, recognising that a collaborative industry will be able to better serve the needs of those persons doing business there, whilst ensuring that the jurisdiction is well equipped to identify, and mitigate against, any associated risks.

This is evident in the approach taken by the Government of the BVI to regulating virtual assets (as detailed further below). The recently introduced Virtual Assets Service Providers Act, 2022 (the "**VASP Act**") (available here: https://www.bvifsc.vg/sites/default/files/virtual_assets_service_providers_act_2022.pdf), which seeks to ensure the BVI's continued compliance with international standards and to adhere to specific recommendations from the Financial Action Task Force in respect of virtual assets, is the result of a public consultation process in which the BVI Financial Services Commission (the "**Commission**") sought the feedback, opinions and comments of all stakeholders.

This key feature of the VASP Act will be discussed in greater detail throughout this chapter. At a high level, however, the VASP Act can be described as a balanced piece of legislation that is proportionate and relevant. Companies engaged in custody and exchange business, which are considered higher risk to end users, attract a higher level of regulatory oversight, whilst other activities, such as innovative technology-based projects and issuances of tokens (an activity that has historically been undertaken by BVI incorporated entities), generally fall outside the VASP Act.

Under the VASP Act, a "virtual asset" is defined as a digital representation of value that can be digitally traded or transferred and can be used for payment or investment purposes. Specifically excluded from this are digital representations of fiat currencies, as well as digital records of credit against a financial institution of fiat currency, securities or other financial assets that can be transferred digitally.

Cryptocurrency regulation

The VASP Act came into force on 1 February 2023. Any entity wishing to provide virtual asset services or to act as a VASP (as defined below) in or from within the BVI is required to be registered by the Commission. Whilst VASPs already operational at the time the VASP Act came into force had until 31 July 2023 to submit an application to the Commission (enabling them to then carry on providing their virtual asset services whilst their application is under review), any new entities must register with the Commission before commencing any of the activities prescribed by the VASP Act.

An application for registration as a VASP must be made in the Commission's approved form specifying the category of VASP registration being applied for, and accompanied by, *inter alia*, (a) a business plan setting out the nature and scale of the virtual asset activities to be conducted, (b) details of the proposed directors, senior officers and compliance officer, including documentation to evidence that they satisfy the Commission's fit and proper criteria, (c) policies and procedures to be adopted by the applicant to meet the obligations under the VASP Act and the AML/CTF/PF legislative regime, and (d) the applicable application fee.

When the Commission approves a VASP application, it will register the applicant, issue a certificate of registration and impose such conditions (if any) on the registration as it considers appropriate (including a requirement to obtain professional indemnity insurance).

The VASP Act defines a "VASP" as a virtual asset service provider who provides, as a business, a virtual asset service and is registered to conduct one or more of the following activities or operations for or on behalf of another person:

- exchange between virtual assets and fiat currencies;
- exchange between one or more forms of virtual assets;
- transfer of virtual assets, where the transfer relates to conducting a transaction on behalf of another person that moves a virtual asset from one virtual asset address or account to another;
- safekeeping or administration of virtual assets or instruments enabling control over virtual assets;
- participation in, and provision of, financial services related to an issuer's offer or sale of a virtual asset; or
- perform such other activity or operation as may be specified in the VASP Act or as may be prescribed by regulations.

A person engaged in any of the following activities or operations, for or on behalf of another person, will be deemed to be carrying on a virtual asset service:

- hosting wallets or maintaining custody or control over another person's virtual asset, wallet or private key;
- providing financial services relating to the issuance, offer or sale of a virtual asset;
- providing kiosks (such as automated teller machines, bitcoin teller machines or vending machines) for the purpose of facilitating virtual asset activities through electronic terminals to enable the owner or operator of the kiosk to actively facilitate the exchange of virtual assets for fiat currency or other virtual assets; or
- engaging in any other activity that, under the Guidelines, constitutes the carrying on of the business of providing a virtual asset service, issuing virtual assets or being involved in virtual asset activity.

Whether an entity is carrying on a virtual asset service will turn on, among other things, whether the asset in question constitutes a "virtual asset". For example, crypto-based derivative products would require more careful consideration and may be caught by one or both the VASP Act or the BVI Securities and Investment Business Act, 2010 ("**SIBA**").

Similarly, consideration should also be given to the list of excluded activities that would take a BVI company outside the scope of the VASP Act, such as providing ancillary infrastructure to allow another person to offer a service, such as a cloud data storage provider or integrity service provider responsible for verifying the accuracy of signatures.

Whilst not intended to regulate cryptocurrency specifically, a BVI entity operating in the cryptocurrency, blockchain technology and Web3 space could also be caught by the BVI's existing regulatory regime, including under:

- the BVI Business Companies Act, 2004 (as amended);
- SIBA (as discussed further below);
- the Financing and Money Services Act, 2009 ("**FMSA**") (as discussed further below);
- the Anti-Money Laundering Regulations, 2008 (as amended) (the "**AML Regs**") (as discussed further below);
- the Anti-Money Laundering and Terrorist Financing Code of Practice (as discussed further below); and
- the Economic Substance (Companies and Limited Partnerships) Act, 2018 (as amended) – this will be of particular relevance if the BVI company is proposing to hold any intellectual property rights in connection with the underlying technology.

To avoid duplication of regulation, the VASP Act does specifically provide that a person registered under the VASP Act who carries on *only* the business of providing a virtual asset service need not be licensed under SIBA or FMSA.

Sales regulation

VASP Act

Under the VASP Act, whilst not expressly excluded, it is generally accepted that the sole act of issuing or selling virtual assets in or from within the BVI is not an activity regulated by the VASP Act in and of itself. However, the provision of financial services related to a virtual asset issuance, as well as the transfer of virtual assets, if being carried out by a BVI entity as a business on behalf of another party, will likely constitute virtual asset services and require that entity to be registered with the Commission under the VASP Act.

SIBA

SIBA regulates, among other things, the provision of investment services from within the BVI. SIBA provides that any person carrying on, or presenting themselves as carrying on, investment business of any kind in or from within the BVI must do so through an entity regulated and licensed by the Commission (subject to the safe harbours in SIBA). Investment business is widely defined and covers: (i) dealing in investments; (ii) arranging deals in investments; (iii) investment management; (iv) investment advice; (v) custody of investments; (vi) administration of investments; and (vii) operating an investment exchange.

"Investments" is also widely defined and may include: (i) shares, interests in a partnership or fund interests; (ii) debentures; (iii) instruments giving entitlements to shares, interests or debentures; (iv) certificates representing investments; (v) options; (vi) futures; (vii) contracts for difference; and (viii) long-term insurance contracts.

Whether a virtual asset falls under the SIBA regime will depend on whether it has characteristics similar to the shares, etc. within the definition of investments.

Additionally, any pooling vehicle that is investing into the virtual asset space, or accepting virtual assets by way of subscription and then investing into more traditional asset classes, would be advised to seek BVI legal advice as to whether such activities would require registration as a fund.

Taxation

The BVI International Tax Authority has not issued any formal statement in relation to the taxation of virtual assets. However, the BVI is a tax-neutral jurisdiction and its income tax is set at 0%, which means that there is no income tax actually levied or paid to the Government of the BVI. As such, there is no requirement for BVI entities to file an income tax return, although they must submit an annual economic substance declaration. In addition, there are no capital gains taxes, gift taxes, profits taxes, inheritance taxes or estate duty in the BVI.

For tax purposes, BVI entities may become resident in any jurisdiction, based on such tests as "management and control". All BVI entities are exempt from tax in the BVI and can obtain a certificate from either the BVI registrar or the Inland Revenue to that effect. Moreover, the BVI operates a source-based tax system under which BVI entities will be taxed in the BVI on their BVI net income after all BVI expenses. Consequently, BVI entities operating outside of the BVI, if tax resident in the BVI, should not have their foreign source income taxed in the BVI.

Where there is an initial token/coin offering, the exchange operators will need to be cognisant of the impact of the Foreign Account Tax Compliance Act ("**FATCA**") and Common Reporting Standards ("**CRS**").

Money transmission laws and anti-money laundering requirements

The relevant money transmittal law in the BVI is FMSA, which regulates money services business. FMSA defines money services business as including:

- automated teller machine services;
- money transmission services;
- cheque exchange services;
- currency exchange services; and
- the issuance, sale or redemption of money orders or travellers' cheques.

Whilst the consensus is that "money" and "currency" refer to fiat currencies rather than cryptocurrencies, the specific exclusion in the VASP Act, noted above, whereby any person registered under the VASP Act to carry on only the business of providing a virtual asset service will be exempt from FMSA, will be of particular relevance, and helps to provide certainty to many virtual asset service providers (for example, those involved in the transfer of virtual assets from one account to another). Care will, however, need to be taken where a company is deemed to be carrying out any activities that fall outside the scope of the VASP Act, as the above-noted exemption would not apply in those circumstances.

Also applicable to VASPs are the Anti-Money Laundering (Amendment) Regulations, 2022 and the Anti-Money Laundering and Terrorist Financing (Amendment) Code of Practice, 2022, which, from 1 December 2022, brought VASPs within scope of the BVI AML/CTF regime for transactions involving virtual assets valued at $1,000 or more.

Although a detailed consideration of the specific requirements of the BVI's AML/CTF regime falls outside the scope of this chapter, any person subject to the regime will generally need to do, among other things, the following:

- appoint a named individual as an AML compliance officer to oversee its adherence to the AML Laws and to liaise with the supervisory authorities (and, under the VASP Act, a VASP must have such officer approved by CIMA);
- appoint a named individual as the money laundering reporting officer to act as a reporting line within the business; and

- implement procedures to ensure that counterparties are properly identified, risk-based monitoring is carried out (with specific regard to the nature of the counterparties, the geographic region of operation, and any risks specifically associated with new technologies such as virtual assets), proper records are kept, and employees are properly trained.

In addition, the Commission has issued the Virtual Assets Service Providers guide to the prevention of money laundering, terrorist financing and proliferation financing (available here: https://www.bvifsc.vg/library/virtual-assets-service-providers-guide-prevention-money-laundering-terrorist-financing-and), and new regulatory requirements have been put in place to ensure that sufficient information is obtained relating to transfers of virtual assets by intermediaries.

In our experience, most parties will be best advised to consult specialist third-party providers to assist with this process.

Promotion and testing

The BVI introduced the Financial Services (Regulatory Sandbox) Regulations, 2020 (the "**Sandbox Regulations**") to encourage technological innovation in the financial technology sector under a lighter touch regulatory regime. The Sandbox Regulations were introduced to assist:

- start-ups that wish to provide new financial services solutions that involve a FinTech business model that is not currently covered (whether explicitly or implicitly) under current BVI legislation;
- start-ups that wish to test innovative technology to deliver a licensable financial service; and
- entities already licensed by the Commission that wish to test an innovative technology as part of their already approved financial service offering.

A person approved under the Sandbox Regulations as a Sandbox participant prior to the VASP Act coming into force can notify the Commission in writing of its intention to provide innovative FinTech in relation to virtual assets (with such notification being treated as an application for registration as a VASP).

Where a VASP that is not registered under the VASP Act or approved under the Sandbox Regulations wishes to carry on a virtual asset service and provide innovative FinTech in accordance with the Sandbox Regulations, it may submit an application to the Commission in accordance with the Sandbox Regulations, with it being noted in the application that it intends to carry on the business of providing virtual asset services in relation to which the innovative FinTech will be applied.

Ownership and licensing requirements

There are no restrictions in the BVI on an investment manager owning cryptocurrencies for investment purposes. Whilst currently untested, due to the infancy of the VASP Act, we would expect that an investment manager may need to apply for registration under the VASP Act in order to hold those virtual assets (if it is determined that the investment manager is holding those virtual assets for and on behalf of a third party). Whether an investment manager that is licensed under the Approved Manager regime would also need to be registered separately under the VASP Act is also yet to be confirmed.

Again, whilst as yet untested, an investment fund incorporated or formed in the BVI that proposes to deal in virtual assets as part of its investment strategy will likely be able to do so

without being registered by the Commission under the VASP Act, provided that it is dealing with those virtual assets on a proprietary basis.

Mining

Mining cryptocurrencies is not within scope of the VASP Act and therefore remains an unregulated activity from a BVI perspective, whether conducted in the BVI or by a BVI company outside of the BVI. The BVI has high electricity costs and as such, mining within the BVI, particularly on a large scale, is unlikely to be efficient.

Border restrictions and declaration

The BVI does not impose any general border restrictions on the ownership or importation of virtual assets.

As part of the BVI's commitment to combatting money laundering and terrorist financing, the Customs Management and Duty Act, 2010 mandates that any person entering or departing the BVI shall make a declaration of anything contained in the person's baggage or carried with the person that, being an amount of cash (which includes coins, notes, travellers' cheques and negotiable instruments such as money orders, cheques, stock and bonds in any currency), exceeds $10,000. Whilst the VASP Act does require that value-based terms contained in any financial services legislation or any other enactment relating to money laundering, terrorist financing and proliferation financing shall be construed to include virtual assets, there is a conceptual question of what would amount to the importation or transportation of such assets given the nature of these assets, particularly those based or recorded on a distributed ledger. As such, we would not expect such a requirement to apply to virtual assets.

Reporting requirements

As noted above, a BVI company providing a virtual asset service in connection with a transaction involving virtual assets valued at $1,000 or more will be deemed to be carrying on a "relevant business" for the purposes of the AML Regs and will be required to comply with the BVI AML/CTF/PF legislative regime, including complying with the "travel rule" and reporting suspicions of money laundering or other criminal activity with the Commission and/or the BVI's Financial Investigation Agency, as applicable.

The OECD has also published a final version of its Crypto-Asset Reporting Framework ("**CARF**") and 2023 update to the CRS, creating a cross-border reporting framework to provide for standardised exchange of information on transactions in crypto-assets. As such, we can expect amendments to be made to the CRS legislative framework in the BVI in order to implement the recommendations under CARF.

Estate planning and testamentary succession

Cryptocurrencies and other virtual assets have not been widely used for the purposes of estate planning and testamentary succession under BVI law.

Neither the VASP Act nor any other particular regime under BVI law deals specifically with the treatment of virtual assets upon the death of an individual holding them. This means that, in principle, and assuming BVI law governs succession to the deceased's estate, virtual assets will be treated in the same way as any other asset.

As is the case in many jurisdictions beyond the BVI, there is likely to be some uncertainty as to where the situs of a virtual asset is located (or indeed whether or not a situs can be determined at all). To the extent that the asset can be analysed under traditional conflict-of-laws rules as sited in the BVI, then a deceased's virtual asset could not be validly transmitted to his/her heirs or beneficiaries until an application is made to the BVI High Court Probate Registry (the "**Registry**"). To deal with a deceased's virtual asset, a person would need to be appointed as legal personal representative of the deceased, by obtaining the appropriate grant from the Registry. There are two types of grant that may be obtained:

- Grant of Probate (where the deceased left a will that expressly deals with the BVI situs virtual asset); and
- Grant of Letters of Administration (where the deceased did not leave a will expressly covering the BVI situs virtual asset).

In respect of the latter, the deceased would be deemed to have died "intestate" in relation to the BVI situs virtual asset – even if they had a valid will covering assets in other jurisdictions.

The main potential difficulty that may arise is practical; namely that anyone inheriting a virtual asset will, on the face of it, often only be able to access that virtual asset if the personal representative of the deceased or the beneficiary (as the case may be) has or can obtain the information needed in order to gain access and control over that virtual asset (e.g. a private key to the wallet in which it is stored). Most exchanges have policies in place to transfer virtual assets to next of kin, but these policies, and the transfer requirements, will vary across exchanges, and it is generally regarded as prudent to avoid leaving significant value on exchanges for any length of time due to the risks of hacking and insolvencies.

Chris Duncan
Tel: +1 345 749 2057 / Email: chris.duncan@careyolsen.com

Chris is in the corporate group of Carey Olsen and a partner of the firm. He advises on the full spectrum of digital assets, cryptocurrency and fintech matters across the Cayman Islands and the British Virgin Islands, from structuring and restructuring to regulatory matters and disputes, and is described by clients in *Chambers FinTech* as being "very familiar with the blockchain/Web3 space and developments in Cayman law". Chris also advises on a broad range of private client matters.

Chris was formerly with Mourant in Guernsey and a large firm in New Zealand. Chris obtained a Bachelor of Laws and a Bachelor of Science (majoring in Chemistry) from the University of Otago in New Zealand.

Katrina Lindsay
Tel: +1 284 346 4032 / Email: katrina.lindsay@careyolsen.com

Katrina is an experienced corporate and finance lawyer and a key member of the firm's growing virtual assets practice. Katrina spent three years in the Carey Olsen Jersey office where she acted on a number of high-profile transactions, including the establishment of the largest real estate fund to be listed on the London Stock Exchange. Katrina relocated to the Carey Olsen BVI office in 2016 and has developed a diverse practice in advising clients from around the globe on BVI corporate, mergers & acquisitions, financing, security enforcement, restructuring and virtual asset-related matters. She is retained as general BVI legal counsel to various publicly listed companies, given the breadth and depth of matters she is able to advise on, and she regularly assists clients in the virtual assets space navigate the evolving regulatory landscape.

Carey Olsen

Rodus Building, P.O. Box 3093, Road Town, Tortola, British Virgin Islands
Tel: +1 284 394 4030 / URL: www.careyolsen.com

Canada

Alix d'Anglejan-Chatillon, Ramandeep K. Grewal & Éric Lévesque
Stikeman Elliott LLP

Government attitude and definition

As in many countries, the regulation of cryptocurrencies in Canada is divided among various levels of government and administrative agencies, depending on the nature of the activity undertaken. Despite these jurisdictional constraints, Canadian regulators generally continue to take a receptive and innovative approach to regulation, including, for example, in approving crypto-based exchange-traded funds ("**ETFs**") and developing a pragmatic regulatory oversight and compliance framework under provincial securities regulation.

Cryptocurrency regulation

Provincial securities and derivatives regulation provides the main regulatory framework for the regulation of digital assets in Canada. As discussed below under "*Money transmission laws and anti-money laundering requirements*", jurisdiction is also exercised by the federal government through federal anti-money laundering legislation, which requires registration of certain virtual currency exchange or transfer services as money services businesses ("**MSBs**").

Securities regulation in Canada generally governs the distribution and trading of both securities and derivatives. These activities are primarily regulated through the imposition of prospectus requirements, dealer, adviser and investment fund manager registration requirements, and certain requirements imposed upon those operating exchanges, alternative trading facilities or other marketplaces that facilitate trading activities, as well as related reporting and disclosure requirements.

The Canadian Securities Administrators (the "**CSA**") is an umbrella organisation of Canada's provincial and territorial securities regulators. While there are no specific rules or regulations for digital assets, the CSA has published guidance in the form of a number of staff notices with respect to virtual currencies with a view to addressing rapidly evolving developments in retail crypto markets and adapting the existing regulatory framework to digital assets. The CSA and the investment industry self-regulatory organisation known as the Canadian Industry Regulatory Organization ("**CIRO**") set out their framework and proposed approach to regulating this asset class in Staff Notice 21-329 – *Guidance for Crypto-Asset Trading Platforms: Compliance with Regulatory Requirements* ("**Staff Notice 21-329**").[1] Staff Notice 21-329 provided an actionable roadmap, building on earlier guidance, including the 2019 Consultation Paper 21-402 – *Proposed Framework for Crypto-Asset Trading Platforms* (the "**Consultation Paper**"),[2] Staff Notice 46-307 – *Cryptocurrency Offerings*,[3] Staff Notice 46-308 – *Securities Law Implications for Offerings of Tokens*,[4] Staff Notice 21-327 – *Guidance on the Application of Securities Legislation to Entities Facilitating the Trading of Crypto Assets* ("**Staff Notice 21-327**"),[5] and Staff

Notice 51-363 – *Observations on Disclosure by Crypto Assets Reporting Issuers*.[6] Virtual currencies may be subject to Canadian provincial securities and derivatives laws to the extent that a virtual currency is considered a security or a derivative for the purposes of those laws, which define a security to include, among other things, an investment contract. The seminal case in Canada for determining whether an investment contract exists is *Pacific Coast Coin Exchange v. Ontario (Securities Commission)*,[7] where the Supreme Court of Canada identified the four central attributes of an investment contract, namely: (a) an investment of money; (b) in a common enterprise; (c) with the expectation of profit; and (d) where this profit is to be derived in significant measure from the efforts of others.

The application of the Pacific Coin test to virtual currencies is not always straightforward, however. Industry participants have taken the position that proper utility tokens, which have a specific function or utility beyond the mere expectation of profit (such as providing their holders with the ability to acquire products or services), should not be considered securities. This position appears to have generally been accepted by the CSA and CIRO. The CSA and CIRO have also acknowledged in the Consultation Paper that it is widely accepted that some of the well-established virtual currency assets that function as a form of payment or a means of exchange on a decentralised network, such as BTC, are not currently, in and of themselves, securities or derivatives and have features that are analogous to commodities such as currencies and precious metals.

In assessing whether a particular virtual currency will be considered a security subject to Canadian securities laws, the CSA has generally applied a very broad and multi-factor approach to determining whether an investment contract exists and focusing on the substance of the virtual currency over its form.

A particular virtual currency that meets the criteria of the Pacific Coin test or has certain of the characteristics described in the CSA guidance may be properly considered an investment contract and therefore a security, subject to Canadian securities laws. A similarly broad approach is generally expected to apply when reviewing non-fungible tokens ("**NFTs**"), including whether there is a capital-raising and/or investment element, how the number of tokens issued correlates to the original purpose, and whether the tokens are expected to trade on secondary markets. More recently, the CSA has expanded its regulatory approach to cover arrangements that are securities or derivatives because they are "crypto contracts" and, as discussed below, the consequences of characterisation as a security or a derivative include distribution-related (prospectus) requirements, as well as requirements to be registered as a dealer and/or marketplace.

The guidance set out in Staff Notice 21-327 further outlines the circumstances in which the CSA will consider "any entity that facilitates transactions relating to cryptoassets" to be subject to securities legislation requirements relating to platform recognition and dealer registration. In particular, the CSA has cautioned that securities legislation may also apply to platforms that facilitate the buying and selling of cryptoassets, including cryptoassets that are commodities, because the user's contractual right to the cryptoasset may itself constitute a derivative. This will generally be the case where the platform is determined to be merely providing users with a contractual right or claim to an underlying cryptoasset, rather than immediately delivering the cryptoasset.

While regulators will consider all the terms of the relevant contract or instrument, the CSA has taken the view that if there is no immediate delivery of the cryptoasset, securities legislation will generally apply. For these purposes, immediate delivery will be considered to have occurred if: (a) there is immediate transfer of ownership, possession and control of

the cryptoasset and the user is free to use, or otherwise deal with, the cryptoasset without any further involvement with, or reliance on, the platform or its affiliates, and the platform or any affiliate retaining any security interest or any other legal right to the cryptoasset; and (b) following the immediate delivery, the user is not exposed to insolvency risk (credit risk), fraud risk, performance risk or proficiency risk on the part of the platform.

Other factors to be considered include: (a) the contractual arrangements between the platform and the user; (b) whether there is immediate settlement of the transaction; (c) whether there is margin and leverage trading; (d) typical commercial practice with regard to immediate delivery; (e) whether there is immediate transfer to a user's wallet; and (f) who has ownership, possession or control over the transferred cryptoasset.

Sales regulation

To the extent that a virtual currency is considered a security or a derivative, the issuance or distribution to the public is subject to prospectus, qualification or similar requirements, or must be effected pursuant to applicable exemptions from prospectus or derivatives qualification requirements.

There are a number of options available for distributing securities in Canada on a prospectus-exempt basis, generally referred to as "exempt distributions" or "private placements". Most of these exemptions are harmonised under National Instrument 45-106 *Prospectus Exemptions*. The CSA has indicated that persons wishing to distribute virtual currencies may do so pursuant to these exemptions.[8]

A number of investment funds have also completed prospectus offerings qualifying the distribution of units of retail pooled fund vehicles whose underlying investments are cryptoassets such as BTC and ETH. The first such offering was completed by 3iQ for its Bitcoin Fund in April 2020 and then in December 2020 for the Ether Fund. CI Galaxy Bitcoin Fund, managed by CI Asset Management, and Bitcoin Trust, managed by Ninepoint Partners LP, were also launched in December 2020 and led to a number of similar offerings of crypto-based ETFs.

Ownership and licensing requirements

Dealer registration

Any person or company engaging in, or holding themselves out as engaging in, the business of trading or advising in securities, and, in certain Canadian jurisdictions, in derivatives, must register as a dealer or as an adviser or, where available, conduct these activities pursuant to an exemption from the dealer or adviser registration requirement under the applicable securities or derivatives laws. A person or entity that directs the business, operations and affairs of an "investment fund" (as defined under applicable laws) must comply with the investment fund manager registration requirement or obtain an exemption from that requirement.

In Canada, the requirement to register as a dealer or an adviser is triggered where a person or company conducts a trading or advising activity with respect to securities or derivatives for a business purpose. The mere holding out, directly or indirectly, as being willing to engage in the business of trading in securities may trigger the requirement to register as a dealer. However, a number of factors must be considered when determining whether registration is required, including whether a business engages in activities similar to a registrant, intermediates or expects to be remunerated or compensated.

In the context of virtual currency distributions, the CSA has noted the following additional factors in determining whether a person or entity may be considered to be trading in securities for a business purpose, namely: (a) soliciting of a broad range of investors, including retail investors; (b) using the internet to reach a large number of potential investors; (c) attending public events to actively advertise the sale of a virtual currency; and (d) raising a significant amount of capital from a large number of investors.

Following the regulatory approach outlined in Staff Notice 21-329, a number of domestic platforms have been granted "restricted dealer" registration while other domestic and global platforms continue to engage with CSA members with a view to being appropriately regulated.[9]

Exchanges and other platforms

As marketplaces, exchanges are regulated pursuant to their applicable provincial securities statutes, as well as under National Instrument 21-101 *Marketplace Operation* ("**NI 21-101**"), National Instrument 23-101 *Trading Rules* ("**NI 23-101**") and their related companion policies.

NI 21-101 defines a marketplace as a facility that brings together buyers and sellers of securities, brings together the orders for securities of multiple buyers and sellers, and uses established non-discretionary methods under which the orders interact with each other. Additional factors apply to further distinguish marketplaces that are exchanges.

To operate as an exchange in Canada, a person or company must first apply for recognition as an exchange or for an exemption from the recognition requirement. As another type of marketplace, alternative trading systems, which provide automated trading systems that match buyer and seller orders, are also regulated under NI 21-101 and NI 23-101.

It follows that exchanges or other platforms that facilitate the purchase, transfer or exchange of virtual currencies that are considered securities or derivatives may be subject to recognition requirements as securities or derivatives exchanges or marketplaces. In the institutional market, prescribed or negotiated exemptions may be available in respect of platform-related recognition requirements under securities or derivatives laws, subject to the satisfaction of certain conditions and acceptance by the applicable regulators.

The appropriate category of dealer platform registration depends on the business model and the nature of the platform's activities. Relevant factors include whether the platform offers margin or leverage.

Dealer platforms that trade crypto contracts and trade or solicit trades for retail investors will generally be expected to be registered as investment dealers and become members of CIRO. However, they are able to access a transitional "interim period" process by seeking "restricted dealer registration" (under the stated guidance, provided they do not offer leverage or margin trading) while they ramp up to full investment dealer registration and compliance. During that period, applicant platforms may expect to undergo a detailed regulatory screening of trade flows, financial controls and auditing, custody, valuation, insurance, market integrity, professional proficiency and experience, ability to comply with prescribed business conduct requirements, cybersecurity and risk management, although some flexibility may be extended. In 2022, significant market volatility and liquidity issues impacting the broader industry led the CSA to introduce a series of additional measures to tighten the conditions for domestic and foreign platforms seeking registration to operate in the Canadian retail market. Expanded commitments were initially imposed in the form of pre-registration undertakings ("**PRUs**"), including enhanced governance, risk management, operational, custodial, insurance, financial reporting and other compliance and reporting requirements.

On February 22, 2023, the CSA announced further restrictive operating conditions for platforms seeking registration in Canada through expanded PRU commitments covering more stringent custody and segregation requirements, prohibitions on pledging, hypothecating or otherwise using custodied assets, new commitments for controlling minds and global affiliates, excluding proprietary tokens from the calculation of regulatory capital, enhanced and more frequent financial reporting, enhanced Chief Compliance Officer ("**CCO**") requirements, and a prohibition on enabling trading in "value-referenced cryptoassets" (commonly referred to as stablecoins) and crypto contracts based on proprietary tokens except with the prior written consent of the CSA.

Platforms that were unable or unwilling to provide an enhanced PRU or implement the necessary system changes within 30 days of the publication of Staff Notice 21-332 (i.e., by March 24, 2023) were expected to take appropriate steps to identify and off-board existing users in Canada, restrict trading access to Canadian-resident users and provide periodic reporting to the CSA.

Asset management and investment funds

Persons and entities operating or administering collective investment structures that hold or invest in virtual currencies may also be subject to investment fund manager registration requirements, in addition to dealer, adviser and prospectus or private placements requirements. The structures themselves may also be subject to reporting and business conduct requirements that apply to investment funds.

Canada has been at the forefront of regulatory and market breakthroughs in the retail crypto fund space. In 2020, Canada's 3iQ launched North America's first major exchange-listed Bitcoin and Ether Funds. In 2021, Canada's Purpose Investments obtained approval from the CSA for the world's first actively managed crypto-based ETFs.

The CSA has since registered several managers of pooled investment vehicles and approved a number of retail closed-end funds and ETFs investing in cryptoassets.

On July 6, 2023, the CSA published Staff Notice 81-336 – *Guidance on Crypto Asset Investment Funds that are Reporting Issuers*, outlining their regulatory expectations with respect to public investment funds holding cryptoassets ("public cryptoasset funds") in light of recent crypto market events. This guidance includes compliance with the regulatory framework generally applicable to publicly distributed investment funds in Canada, the market characteristics of portfolio cryptoassets, liquidity, valuation and custodial practices, issues relating to staking and other high-yield generation activities, and know-your-client, know-your-product and suitability requirements. The CSA guidance notes that as of April 30, 2023, there were 22 public cryptoasset funds in Canada that collectively had approximately C$2.86 billion in net assets.

Promotion and testing

The CSA and CIRO have addressed promotional activities in Joint Staff Notice 21-330 – *Guidance for Crypto-Trading Platforms; Requirements relating to Advertising, Marketing and Social Media Use* issued on September 23, 2021, including requirements, best practices and examples with respect to advertising, marketing, social media activities, fee disclosure and other compliance matters for crypto-trading platforms under Canadian securities legislation.

The CSA has also established a regulatory sandbox initiative to support fintech businesses seeking to offer innovative products, services and applications in Canada. It allows firms to register and/or obtain exemptive relief from securities laws requirements under what

is stated to be "*a faster and more flexible process than through a standard application, in order to test their products, services and applications throughout the Canadian market on a time limited basis*". Certain provincial securities regulators have established their own specifically tailored programmes, such as Ontario Securities Commission's Launchpad, *Autorité des marchés financiers*' Fintech group and fintech lab, British Columbia Securities Commission's Fintech Advisory Forum and Advertising Standards Canada's InnoFinTeam.

Money transmission laws and anti-money laundering requirements

Under the federal *Proceeds of Crime (Money Laundering) and Terrorist Financing Act* (Canada) (the "**PCMLTFA**"), any entity that is engaged in the business of foreign exchange dealing, remitting or transmitting funds, issuing or redeeming money orders or similar instruments, dealing in virtual currency or providing crowdfunding platform services, must be registered in Canada as an MSB. Under guidance issued by the Financial Transactions and Reports Analysis Centre of Canada ("**FINTRAC**"),[10] any entity that holds a permit, licence or registration related to any of these services, advertises by any means that it is engaged in providing any of these services, or reports income from any of these services as income from a separate business, must also register as an MSB. Any entity that does not have a place of business in Canada (which includes having employees, agents or branches in Canada), and directs any of the above services at, and provides these services to, persons or entities in Canada, must also be registered as a foreign money services business ("**FMSB**"). Both domestic and foreign MSBs must implement a compliance programme to implement know-your-customer, reporting, record-keeping, travel rule and related compliance requirements under the PCMLTFA.

The activities that are considered "dealing in" virtual currency are not specifically defined in the legislation. However, FINTRAC has clarified that these activities include virtual currency exchange services and virtual currency transfer services, with a view to regulating entities such as virtual currency exchanges, and not individuals or businesses that use virtual currency for buying and selling goods and services. A "virtual currency exchange transaction" is defined in this guidance as an exchange, at the request of another person or entity, of virtual currency for funds, funds for virtual currency or one virtual currency for another. Virtual currency transfer services include transferring virtual currency at the request of a client or receiving a transfer of virtual currency for remittance to a beneficiary. An entity registered as the equivalent of an MSB and/or performing any of the covered services may also be required to be registered as an FMSB in Canada.

Under FINTRAC guidance, a business is considered to be "directing services" at persons or entities in Canada if: (a) the business's marketing or advertising is directed at persons or entities located in Canada (e.g., in Canadian newspapers and on websites aimed at clients in Canada or through emails to persons in Canada promoting its virtual currency services); (b) the business operates a ".ca" domain name; or (c) the business is listed in a Canadian business directory.

However, FINTRAC guidance also provides that even if none of the above factual elements apply, a business may still be directing services at persons or entities in Canada, and a combination of additional criteria should also be considered in order to make this determination, including: (a) describing services as being offered in Canada; (b) offering products or services in Canadian dollars; (c) making customer service support available in Canada; (d) seeking feedback from clients in Canada; and (e) having another business in Canada promote its services to clients in Canada.

These criteria are not exhaustive and apply regardless of whether a Canadian client to whom the services are directed is an individual or an institutional client. FINTRAC guidance provides that a client is deemed to be "in Canada" if they have a connection or residential ties with Canada (such as having an address in Canada), the document or information used to verify the client's identity is issued by a Canadian province or territory or by the federal government, or their banking, credit card or payment processing service is based in Canada. Failure to comply with applicable requirements of the PCMLTFA may result in criminal charges for non-compliance offences or administrative monetary penalties.

Canadian federal law also includes other laws and regulations governing money laundering, terrorist financing and the use/handing of proceeds of crime, and various trade sanction and similar restrictions. These rules may provide additional monitoring and reporting obligations and prohibitions, including offences such as knowingly collecting or providing funds to terrorist organisations or associated individuals, or otherwise dealing with sanctioned governments, entities or individuals. The rules generally apply to persons in Canada and Canadians outside of Canada.

Québec is the only provincial jurisdiction to have implemented similar legislation, the *Money-Services Businesses Act* (Québec) (the "**QMSBA**"), requiring MSB registration. The QMSBA is administered by Revenu Québec, the taxation authority in that province. Unlike the PCMLTFA, the QMSBA does not distinguish between foreign and domestic MSBs. On March 29, 2023, the British Columbia government also introduced legislation that will similarly require MSBs to register provincially with the BC Financial Services Authority ("**BCFSA**"). This legislation is not yet in force.

Reporting requirements

MSBs and FMSBs are subject to prescribed suspicious transaction reporting, terrorist property reporting, large cash transaction reporting, large virtual currency transaction reporting and electronic funds transfer ("**EFT**") reporting requirements. MSBs and FMSBs must take reasonable measures to ensure that prescribed travel information is included in relation to virtual currency and EFT transfers.

Border restrictions and declaration

There are no border restrictions specific to cryptocurrencies, but persons entering or leaving Canada with C$10,000 or more in their possession must report it in person on *E677 – Cross-Border Currency or Monetary Instruments Report – Individual* in the case of persons reporting their own currency or monetary instruments, or *E667 – Cross-Border Currency or Monetary Instruments Report – General* in the case of persons transporting them for a third party. Canadian tax reporting requirements may also apply.

Mining

The process of virtual currency mining, which employs specialised, high-speed computers, is energy intensive. However, Canada's cold temperatures and low electricity costs make it particularly attractive for virtual currency miners.[11] While virtual currency mining is not specifically regulated in Canada at this time, the use of virtual currency mining hardware may be subject to provincial and municipal requirements relating to the use of energy. On March 9, 2022, the Ontario Ministry of Energy tabled regulatory amendments to Ontario Regulation 429/04 that would prevent facilities that engage in cryptocurrency mining from participating in the Industrial Conservation Initiative ("**ICI**")[12] on the basis that virtual currency mining is energy intensive and runs counter to ICI's goals.[13]

The increased demand for electricity in this sector and concerns over related environmental impacts have also led certain provincial and municipal governments to pause virtual mining applications. In 2022, the governments of Manitoba and British Columbia introduced moratoriums on new crypto mining connections to provincial hydroelectric grids over environmental concerns.[14] In January 2023, at the request of Hydro Québec, Québec's *Régie de l'énergie* (energy board) approved a suspension of the process for allocating capacity dedicated to cryptographic use applied to blockchains while its request concerning the reassessment of the number of megawatts involved is being processed. Any new crypto mining project in Québec that involves utilisation of at least 50 kilowatts ("**kW**") of installed capacity for cryptographic use applied to blockchains is now subject to the price of 16.603¢/kWh specified in Rate CB with regard to energy consumption.[15]

Taxation

Taxation of virtual currencies

For Canadian tax purposes, the Canada Revenue Agency (the "**CRA**") has taken the position that virtual currencies constitute a commodity rather than a currency.[16] Gains or losses resulting from the trade of virtual currencies are therefore taxable either as income or capital for the taxpayer.[17] The treatment of a transaction as being taxable as income or capital is a question of fact and is determined by the CRA through an examination of the nature of the relevant transaction. Where a transaction is considered on capital account, the taxpayer will be required to include, in computing its income for the taxation year of disposition, one-half of the amount of any capital gain (a taxable capital gain) realised in that year. Subject to and in accordance with the provisions of the *Income Tax Act* (the "**ITA**"),[18] the taxpayer will generally be required to deduct one-half of the amount of any capital loss (an allowable capital loss) realised in the taxation year of disposition against taxable capital gains realised in the same taxation year. Allowable capital losses in excess of taxable capital gains for the taxation year of disposition generally may be carried back and deducted in any of the three preceding taxation years or carried forward and deducted in any subsequent taxation year against net taxable capital gains realised in those taxation years, to the extent and under the circumstances specified in the ITA. Where a transaction is considered on income account, the resulting gains are taxed as ordinary income and the losses are generally deductible.

Recently, the CRA published a tax tip stating that taxpayers should keep proper financial records of all of their cryptocurrency transactions, including when they purchase, dispose, or mine cryptocurrency.[19]

Virtual currency mining

The tax treatment of virtual currency mining turns on whether the activity is undertaken for profit or as a personal endeavour.[20] A personal endeavour is an activity undertaken for pleasure and does not constitute a source of income for tax purposes, unless it is conducted in a sufficiently commercial and business-like way. However, the mining of virtual currencies is likely to be considered a business activity by the CRA given the complexity of the activity. The mining of virtual currencies would therefore require the taxpayer to compute and report business income in compliance with the ITA, including the rules with respect to inventory. The CRA has specifically stated that Bitcoin received by a miner to validate transactions is consideration for services rendered by the miner.[21] Where a taxpayer is in the business of Bitcoin mining, the Bitcoin received must be included in the taxpayer's income at the time it is earned. The CRA has confirmed that the miner must include as income the value of the

services rendered or the value of the Bitcoin received, whichever is more readily valued. The CRA generally expects the value of the Bitcoin received to be more readily valued and, accordingly, this is the amount to be included as income.[22]

Paying with virtual currencies

Where a virtual currency is used as payment for salaries or wages, the amount must generally be included in the employee's income computed in Canadian dollars.[23] As a result of the qualification of virtual currencies as a commodity, the use of virtual currencies to purchase goods or services is subject to the rules applicable to barter transactions. Therefore, where virtual currencies are used to purchase goods or services, the value in Canadian dollars of the goods or services purchased must be included in the seller's income for tax purposes, rather than the value of the virtual currencies.[24] However, the CRA has stated that the fair market value of the virtual currency at the time the supply is made must be used to determine the goods and services tax ("**GST**") and harmonised sales tax ("**HST**") payable on the purchase of a taxable supply of a good or service.[25]

Specified foreign property

The CRA has stated that virtual currencies situated, deposited or held outside Canada fall within the definition of specified foreign property, as defined in the ITA.[26] As such, Canadian residents must report to the CRA when the total costs of virtual currencies situated, deposited or held outside Canada exceed C$100,000 at any time in the year by filing Form T1135 with their income tax return for the year. The CRA has not yet adopted a position on the situs of virtual currencies, which remains an open question, and the issue is currently under review.[27]

Collection of GST and HST on virtual currency transactions

The exchange of cryptocurrency is no longer considered a sale of an asset, but rather a sale of a financial instrument for purposes of GST/HST. Section 123(1) of the *Excise Tax Act* (Canada) (the "**ETA**")[28] includes "virtual payment instruments" to the definition of "financial instruments", rendering any sale of or transaction involving virtual currencies as a form of payment exempt from GST/HST collection.

The Department of Finance sought to clarify the characterisation of cryptoasset activities by introducing Bill C-47, the *Budget Implementation Act*, Bill C-47, on April 20, 2023, which, among other things, proposes to amend the ETA[29] to include cryptoasset mining. With this change, cryptoasset mining would not be considered a supply, so GST/HST would not apply to hashpower services and input tax credit would not be available to the person providing the service. The Department of Finance also proposed in Bill C-47 an amendment to Section 188.2 of the ETA to expand who is involved in a mining activity to not give rise to an input tax credit. The new section is effective as of February 5, 2022. For instance, the allowance of computing resources from one person to another for the purpose of mining will be considered a "mining activity". However, in a situation where the provider of the mining activity is a particular person and the recipient of such activity is known, subsection 188.2(5) of the ETA may provide an exception and supplies of such activities would be taxable supplies and expenses.

Other Canadian legislative requirements

Depending on the specificities of a particular business model and its nexus to the Canadian market, trading, lending and other activities involving crypto contracts may be subject to a

range of other Canadian legal requirements that are not specifically described in this chapter but should be considered, including the potential application of federal banking legislation, provincial loan and trust regulation, consumer protection legislation, privacy legislation, proposed new retail payments legislation, Canadian trade and economic sanctions, extra-provincial business registration, advertising and marketing laws, Canadian anti-spam laws and Québec language laws.

* * *

Endnotes

1. Canadian Securities Administrators, Staff Notice 21-329 – *Guidance for Crypto-Asset Trading Platforms: Compliance with Regulatory Requirements* (Canadian Securities Administrators, 2021) (Staff Notice 21-329).
2. Canadian Securities Administrators and Investment Industry Regulatory Organization of Canada, Consultation Paper 21-402 – *Proposed Framework for Crypto-Asset Trading Platforms* (Canadian Securities Administrators and Investment Industry Regulatory Organization of Canada, 2019) (the Consultation Paper).
3. Canadian Securities Administrators, Staff Notice 46-307 – *Cryptocurrency Offerings* (Canadian Securities Administrators, 2017) (Staff Notice 46-307).
4. Canadian Securities Administrators, Staff Notice 46-308 – *Securities Law Implications for Offerings of Tokens* (Canadian Securities Administrators, 2018).
5. Canadian Securities Administrators, Staff Notice 21-327 – *Guidance on the Application of Securities Legislation to Entities Facilitating the Trading of Crypto Assets* (Canadian Securities Administrators, 2020) (Staff Notice 21-327).
6. Canadian Securities Administrators, Staff Notice 51-363 – *Observations on Disclosure by Crypto Assets Reporting Issuers* (Canadian Securities Administrators, 2021) (Staff Notice 51-363).
7. *Pacific Coast Coin Exchange v. Ontario (Securities Commission)* [1978] 2 SCR 112, which is itself based on the better known "*Howey* Test" set out by the Supreme Court of the United States in *SEC v. W.J. Howey Co.*, 328 U.S. 293 (1946).
8. Staff Notice 46-307.
9. See "*Registered cryptoasset trading platforms*", Ontario Securities Commission (https://www.osc.ca/en/industry/registration-and-compliance/registered-crypto-asset-trading-platforms).
10. The Financial Transactions and Reports Analysis Centre of Canada (the "**FINTRAC**") is Canada's financial intelligence unit and is responsible for monitoring compliance, enforcement and registration under the PCMLTFA. The FINTRAC guidance can be found here: https://www.fintrac-canafe.gc.ca/msb-esm/intro-eng
11. Naomi Powell, "*Crypto-miners flood into Canada, boosting the hopes of small towns looking for a break*", *Financial Post*, June 23, 2020.
12. Ontario Regulatory Registry, "*Industrial Conservation Initiative Cryptocurrency Mining Exclusion*", March 23, 2022.
13. *Ibid*.
14. Manitoba Hydro, "*Province directs Manitoba Hydro to pause new cryptocurrency connections*", November 28, 2022 and Government of British Columbia, "*Province hits pause on electrical connections for cryptocurrency mining*", December 21, 2022.
15. Hydro Québec, Québec's blockchain industry, Allocation of the block of electricity dedicated to cryptographic use.

16. Canada Revenue Agency, Document No. 2013-051470II7, December 23, 2013.
17. Canada Revenue Agency, Compliance, Virtual Currency, last modified June 26, 2019.
18. *Income Tax Act*, RSC 1985, c.1.
19. Canada Revenue Agency, "*Keeping records of your cryptocurrency transaction*", March 27, 2023.
20. Canada Revenue Agency, Document No. 2014-0525191E5, March 28, 2014.
21. Canada Revenue Agency, Document No. 2018-077666II7, August 8, 2019.
22. *Ibid*.
23. Canada Revenue Agency, Compliance, Virtual Currency, last modified June 26, 2019.
24. *Ibid*., footnote 113.
25. *Ibid*.
26. Canada Revenue Agency, Document No. 2014-0561061E5, April 16, 2015.
27. Canada Revenue Agency, Document No. 2022-0936241C6, October 7, 2022.
28. *Excise Tax Act*, RSC 1985, c. E-15.
29. *Budget Implementation Act*, Bill C-47, 1st Session, 44th Parliament, Canada, 2021–2022–2023.

Alix d'Anglejan-Chatillon
Tel: +1 514 397 3240 / Email: adanglejan@stikeman.com

Alix d'Anglejan-Chatillon is a partner and co-head of the Financial Products & Services Group at Stikeman Elliott. She practises principally in the areas of investment management, the regulation of capital markets and derivatives. Her clients include North American, European, and Asian-based investment fund managers, including managers of mutual funds, pooled funds, hedge funds, credit funds, private equity, real estate and infrastructure funds, and fund of fund structures, as well as commercial and investment banks, investment advisers, broker-dealers and other financial sector stakeholders. Alix regularly advises on emerging regulatory issues relating to financial markets infrastructure and trading platforms, cryptoasset and blockchain technology and transactions, fintech solutions and other digital financial products and technologies. She is a member of the International Bar Association and the American Bar Association.

Ramandeep K. Grewal
Tel: +1 416 869 5265 / Email: rgrewal@stikeman.com

Ramandeep K. Grewal is a partner and member of the Corporate Group at Stikeman Elliott. She practises principally in corporate finance and M&A, having expertise on a wide range of matters including securities offerings, corporate governance, and securities regulatory compliance. Raman has counselled Canadian and international issuers and underwriters on a wide range of capital markets transactions and securities regulatory matters, including boards of directors, public and private issuers, dealers, advisers, investment funds and asset managers. She also advises on capital market infrastructure and compliance, including fintech and other capital market developments. Raman is a member of the Canadian Bar Association and the American Bar Association and has recently completed her mandate as a member of the Securities Advisory Committee of the Ontario Securities Commission.

Éric Lévesque
Tel: +1 514 397 2415 / Email: erlevesque@stikeman.com

Éric Lévesque is a partner and member of the Tax Group at Stikeman Elliott. He provides tax and legal advice on Canadian and cross-border M&A. An important part of his practice also involves advising Canadian pension funds on their various investments and he has worked closely on the tax aspects of setting up various investment funds. Éric is a member of the *Association de la planification fiscale et financière* (APFF), of the Canadian Tax Foundation (CTF), and of the International Fiscal Association, Canadian Branch.

Stikeman Elliott LLP

5300 Commerce Court West, 199 Bay Street, Toronto, Ontario M5L 1B9, Canada
Tel: +1 416 869 5500 / Fax: +1 416 947 0866 / URL: www.stikeman.com

Cayman Islands

Chris Duncan & Alistair Russell
Carey Olsen

Government attitude and definition

The Cayman Islands is a leading global financial centre and has developed a reputation as one of the world's most innovative and business-friendly places to operate. The jurisdiction offers a stable society and political system, judicial and legislative links to the United Kingdom, tax neutrality, sophisticated service providers, and a proportionate regulatory regime that focuses closely on the financial services industry, and in particular those catering to sophisticated and institutional investors based elsewhere.

It is this reputation and these attributes that have helped the jurisdiction become an obvious choice for many of those proposing to establish fintech-related structures, whether it be in the form of a fund vehicle investing into digital assets, an exchange or initial coin or token offering, or the launch of a decentralised finance protocol or network.

Each of the Cayman Islands Government, the Cayman Islands Monetary Authority ("**CIMA**"), and industry bodies such as Cayman Finance and the Cayman Islands Blockchain Foundation, acknowledge the importance of continuing to attract fintech and digital assets business to the jurisdiction and ensuring the further growth of the sector. They are also aware, however, of the need to balance this approach with maintaining the Cayman Islands' commitment to the highest standards of financial probity and transparency and the specific considerations that can accompany digital assets.

Consequently, in May 2020, recognising the newly adopted international standards set by the Financial Action Task Force, a new framework for the supervision and regulation of virtual asset services businesses was introduced in the Cayman Islands, namely the Virtual Asset (Service Providers) Act,[1] 2020 (the "**VASP Act**"). The features of the VASP Act are described further in this chapter. However, it is important to note that at the time of writing, this new legislation is only partially in force; the VASP Act is being introduced in two phases, with the first primarily dealing with anti-money laundering ("**AML**") regulations and requiring virtual asset service providers ("**VASPs**") to be registered, and the second phase dealing with licensing and other matters. A specific date for implementation of phase two of the VASP Act has not yet been announced, but it is expected to be in the near term.

Overall, the new framework continues to make the Cayman Islands an attractive jurisdiction for virtual asset services businesses, as it provides a flexible regulatory foundation with a great deal of certainty for those wishing to operate in the space, while furthering Cayman's commitment to international standards.

Under the VASP Act, a "virtual asset" is broadly defined as a digital representation of value that can be digitally traded or transferred and can be used for payment or investment purposes. Specifically excluded from this are digital representations of fiat currencies, as well as "virtual service tokens", which are digital representations of value that are *not*

transferrable or exchangeable with a third party at any time (including digital tokens whose sole function is to provide access to an application or service or to provide a service or function directly to its owner).

To provide further clarity on the VASP Act, the Virtual Assets (Service Providers) Regulations (the "**VASP Regulations**") were introduced in October 2020. The VASP Regulations include the registration application requirements and details of fees as well as providing some further guidance as to virtual asset issuances (as discussed further below).

Cryptocurrency regulation

The VASP Act clearly establishes the legitimacy of digital assets and cryptocurrencies in the Cayman Islands and regulates businesses providing services related to virtual assets. Virtual assets themselves and parties dealing with virtual assets for their own purposes are generally not subject to specific regulation in the Cayman Islands.

Under the VASP Act, all VASPs are required to be licensed or registered with CIMA, obtain a waiver or hold a sandbox licence. A "VASP" is an entity that is incorporated or registered in the Cayman Islands and that provides a virtual asset service as a business or in the course of business.

A "virtual asset service" for this purpose means the issuance of virtual assets or the business of providing any of the following services or operations for or on behalf of another person or entity:

(a) exchange between virtual assets and fiat currencies;
(b) exchange between one or more other forms of convertible virtual assets;
(c) transfer of virtual assets;
(d) virtual asset custody service, which is the business of safekeeping or administration of virtual assets or the instruments that enable the holder to exercise control over virtual assets; or
(e) participation in, and provision of, financial services related to a virtual asset issuance or the sale of a virtual asset.

Cryptocurrency and other digital asset businesses that are not caught by any of the above categories may still be subject to regulation in the Cayman Islands that does not specifically target digital assets, such as the Securities Investment Business Act ("**SIBA**"), the Money Services Act and AML regulations (each described further below).

Sales regulation

VASP Act

As set out above, the issuance of virtual assets, the provision of financial services related to a virtual asset issuance or the sale of a virtual asset, as well as the transfer of virtual assets, if being carried out by a Cayman Islands entity as a business on behalf of another party, will likely constitute virtual asset services and require a licence or registration with CIMA under the VASP Act.

Under the VASP Act, any issuance of virtual assets requires CIMA's prior approval. For this purpose, an issuance means the sale of newly created virtual assets to the public in exchange for fiat currency, other virtual assets or other consideration. "Public" is not defined in the VASP Act so should be interpreted broadly for this purpose; however, helpfully the VASP Regulations distinguish a "private sale", broadly defined as a sale that is not advertised and is sold to a limited number of persons by private agreement from a sale to the public (meaning that registration under the VASP Act may not be required for certain sales). The

sale of virtual service tokens will also be excluded from this requirement and any transfer that is not for consideration (e.g. an "airdrop") should be excluded.

Direct issuances will be subject to a prescribed maximum threshold, which, at the time of writing, has not been fixed. The threshold will not apply where the issuance is facilitated by way of one or more virtual asset trading platforms or obliged entities, provided that the relevant platforms are either licensed under the VASP Act or regulated in another non-high-risk jurisdiction.

Investment funds

An entity that operates as an investment fund that is formed or registered in the Cayman Islands and that issues digital assets may come within the ambit of the Mutual Funds Act (for open-ended funds) or the Private Funds Act (for closed-ended funds), and be required to obtain a registration or licence thereunder to the extent such digital assets constitute equity or investment interests. This will of course depend on a number of aspects, including the terms of the issue and the nature of the assets, and specific advice should be sought. For example, under the Mutual Funds Act, the definition of "equity interest" has recently been amended to include "any other representation of an interest", which is likely broad enough to capture a variety of forms of digital asset.

Additionally, any pooling vehicle that is investing into the digital asset space, or accepting digital assets by way of subscription and then investing into more traditional asset classes, would be advised to seek Cayman Islands legal advice on the point.

Securities Investment Business Act

Pursuant to SIBA, an entity formed or registered in, or that is operating from, the Cayman Islands that engages in dealing, arranging, managing or advising on the acquisition or disposal of digital assets, may come within the ambit of SIBA and be required to obtain a registration or licence from CIMA thereunder (which may be in addition to a registration or licence required under the VASP Act). This applies to the extent that the relevant digital assets constitute "securities" for the purposes of SIBA.

Notably, the definition of "securities" thereunder includes virtual assets that can be sold, traded or exchanged immediately or at any time in the future and that (i) represent or can be converted into another form of traditional securities (e.g. equity interests, debt instruments, options or futures), or (ii) represent a derivative of traditional securities. Consequently, consideration will need to be given on a case-by-case basis as to whether the digital asset in question falls within one of the above categories.

Offerings within the Cayman Islands

In relation to the offering, sale, or issuance of interests within the Cayman Islands, certain regulatory provisions should be borne in mind. For example, the Companies Act prohibits any exempted company formed in the Cayman Islands and not listed on the Cayman Islands Stock Exchange from offering its securities to the Cayman Islands public. The Limited Liability Companies Act includes a similar prohibition in relation to limited liability companies ("**LLCs**"). Even persons based, formed or registered outside the Cayman Islands should be careful not to undertake any activities in relation to a sale or issuance of digital assets that would constitute "carrying on a business" in the Cayman Islands. To do so may entail various registration and licensing requirements and financial and criminal penalties for those who do not comply. There is no explicit definition of what will amount to "carrying on a business" for these purposes and, consequently, persons who propose to undertake concerted marketing to the Cayman Islands public, particularly if it involves engaging in any physical activity in the Cayman Islands, are encouraged to seek specific legal advice.

In practice, however, these restrictions do not generally pose a significant practical concern for issuers given that:

(i) the "public" in this instance is taken to exclude other exempted companies, exempted limited partnerships, and LLCs (which together comprise the majority of Cayman Islands entities); and

(ii) issuers' target investors tend not to include other persons physically based in the Cayman Islands.

Taxation

There are no income, inheritance, gift, capital gains, corporate, withholding or other such taxes imposed by the Cayman Islands Government, including with respect to the issuance, holding, or transfer of digital assets.

Stamp duty may apply to original documents that are executed in the Cayman Islands or are brought into the Cayman Islands following execution. However, the sums levied are generally of a nominal amount.

Entities formed or registered in the Cayman Islands may apply for and, upon the payment of a fee of a relatively small fee, receive a tax exemption certificate confirming that no law enacted in the Cayman Islands after the date thereof imposing any tax to be levied on profits, income, gains or appreciations shall apply to such entity or its operations. Such certificates will generally apply for a period of between 20 and 50 years (depending on the type of entity).

Money transmission laws and anti-money laundering requirements

Money transmission laws

Pursuant to the Money Services Act, any person carrying on a "money services business" in or from the Cayman Islands must first obtain a licence from CIMA thereunder. Any breach of this requirement will constitute a criminal offence.

For the purposes of the foregoing, a "money services business" means the business of providing, among other things, money transmission or currency exchange services.

Although there is no clear authority on the extent to which the foregoing would be seen to include such transactions in cryptocurrency or other digital assets, a cautious and substantive reading of the statute may, in some cases, warrant it. In particular, if the digital assets in question are primarily used to facilitate the transfer of fiat currency from one party to another, or the conversion between fiat currencies, the legislation may well apply. Consequently, persons wishing to establish such businesses are encouraged to consider closely the application of the Money Services Act and consult appropriate advisors.

Anti-money laundering requirements

The very nature and, in some cases, the intended features of digital assets can present heightened compliance risks and practical hurdles to addressing the same. Such features may include the lack of a trusted central counterparty, increased anonymity, and ease of cross-border transfer without any gating or restriction.

Consequently, the Cayman Islands authorities have maintained a keen focus on balancing the jurisdiction's long track record of innovation and the promotion of a business-friendly environment with its commitment to the prevention of crime and maintaining robust standards of transparency. In general, this has been done not by establishing an entirely separate regime for digital assets, but by applying the purposive approach enshrined within the existing framework, which focuses on the specific activity and the nature of the assets in question so as to properly quantify the risk that the same may be used to facilitate illegal activity.

Pursuant to the provisions of the Proceeds of Crime Act, the Anti-Money Laundering Regulations, and the guidance notes thereon (together, the "**AML Laws**"), any persons formed, registered or based in the Cayman Islands conducting "relevant financial business" are subject to various obligations aimed at preventing, identifying, and reporting money laundering and terrorist financing.

"Relevant financial business" is defined in the Proceeds of Crime Act and includes the provision of virtual asset services (which is defined slightly differently for this purpose than under the VASP Act).

Although a detailed consideration of the specific requirements of the AML Laws falls outside of the scope of this chapter, any person subject to the regime will generally need, among other things, to do the following:

- appoint a named individual as an AML compliance officer to oversee its adherence to the AML Laws and to liaise with the supervisory authorities (and, under the VASP Act, a VASP must have such officer approved by CIMA);
- appoint named individuals as the money laundering reporting officer and a deputy for the same to act as a reporting line within the business; and
- implement procedures to ensure that counterparties are properly identified, risk-based monitoring is carried out (with specific regard to the nature of the counterparties, the geographic region of operation, and any risks specifically associated with new technologies such as virtual assets), proper records are kept, and employees are properly trained.

In addition, CIMA has issued specific AML-related guidance for VASPs, and new regulatory requirements have been put in place to ensure sufficient information is obtained relating to transfers of virtual assets by intermediaries.

In our experience, most parties will be best advised to consult specialist third-party providers to assist with this process.

Promotion and testing

Sandbox licences

The VASP Act has introduced a sandbox licence, intended for providers of virtual asset services or other fintech services that utilise innovative technology or use an innovative method of delivery. A sandbox licence provides flexibility, such that CIMA can impose additional requirements or allow certain exemptions, to cater for the relevant business.

Sandbox licences will be temporary, available for a maximum of one year, during which we anticipate that CIMA will assess how best to regulate the business in the future, including whether that requires legislative change, to further promote and monitor the use of the relevant innovation. Further details as to eligibility are not yet available.

Special Economic Zone

Additionally, the Cayman Islands Government has been active in promoting the Special Economic Zone (the "**SEZ**") to those wishing to develop fintech-related products from the jurisdiction.

The SEZ offers businesses focused on the fintech industry the opportunity to establish physical operations within the Cayman Islands in a more streamlined manner. It provides several benefits, including a simpler, more rapid and cost-effective work permit process, concessions with respect to local trade licences and ownership requirements, the ability to be operational within four to six weeks, and allocated office space.

When coupled with the other benefits of the jurisdiction and its recently updated intellectual property laws, the SEZ has proven highly popular with the fintech industry, with the number of blockchain-focused companies established within it continuing to grow.

Ownership and licensing requirements

The Cayman Islands does not impose any restrictions or licensing requirements that are specifically targeted at the ownership, holding or trading of digital assets by those doing so for their own account.

As described above, under the VASP Act, all VASPs (as defined above) are required to be licensed or registered with CIMA, obtain a waiver or hold a sandbox licence. The applicability of other regulatory regimes, such as the Mutual Funds Act and SIBA (each as further detailed above), should also be considered.

Pursuant to the VASP Act, a VASP is required to ensure that its beneficial owners are approved by CIMA as fit and proper persons to have such control or ownership. Subject to possible exceptions for publicly traded companies, ownership interests or voting rights totalling 10% or more in a VASP cannot be issued or voluntarily transferred without CIMA's prior approval.

Mining

The mining of digital assets is not regulated or prohibited in the Cayman Islands currently, nor will it (in and of itself) be regulated or prohibited under the VASP Act. We would note, however, that the import duties applicable to computing equipment and the high cost of electricity production in the Cayman Islands are likely to present practical deterrents to the establishment of any material mining operations within the jurisdiction. It is possible that the increased availability of renewable energy options, and the falling price of the same, may mitigate this somewhat in the future.

Border restrictions and declaration

The Cayman Islands does not impose any general border restrictions on the ownership or importation of digital assets.

As part of the Cayman Islands' commitment to combatting money laundering and terrorist financing, the Customs (Money Declarations and Disclosures) Regulations mandate that individuals transporting money amounting to CI$15,000 (approximately US$18,292) or more into the Cayman Islands must make a declaration in writing to customs officers at the time of entry. However, the Customs Act defines "money" as being confined to cash (i.e. bank notes or coins that are legal tender in any country) and bearer-negotiable instruments (i.e. travellers' cheques, cheques, promissory notes, money orders). As such, we would not expect such a requirement to apply to virtual assets or any other type of digital asset. Further, given the nature of these assets, particularly those based or recorded on a distributed ledger, there is a conceptual question of what would amount to the importation or transportation of such assets.

Reporting requirements

VASPs registered or licensed under the VASP Act will be required to:

- prepare audited accounts and submit them to CIMA annually;
- obtain prior approval from CIMA to appoint senior officers or AML compliance officers;
- provide certain notices to CIMA confirming compliance with AML Laws and data protection laws and ensuring that all communications relating to the virtual asset service are accurate;

- undertake audits of their AML systems and procedures at the request of CIMA; and
- notify CIMA of any licence or registration in another jurisdiction or the opening of an office or establishment of a physical presence in another jurisdiction, the holding or acquisition of a controlling interest in another person engaged in virtual asset service.

Additional reporting and other requirements may apply and may be imposed, which in some cases differ based on the type of virtual asset service being provided.

To the extent that any payment or transfer is made in the context of the conduct of a "relevant financial business" for the purposes of the AML Laws, there may of course be an obligation to make certain filings or reports in the event that there is a suspicion of money laundering or other criminal activity.

Estate planning and testamentary succession

Neither the VASP Act nor any other particular regime under Cayman Islands law deals specifically with the treatment of virtual assets upon the death of an individual holding them. This means that, in principle, and assuming Cayman Islands law governs succession to the deceased's estate, virtual assets will be treated in the same way as any other asset and may be bequeathed to beneficiaries in a will, or, if a person dies intestate, will be dealt with under the intestacy rules in the Cayman Islands Succession Act.

As is the case in many jurisdictions beyond the Cayman Islands, there is likely to be some uncertainty as to where the *situs* of a virtual asset is located (or indeed whether or not a *situs* can be determined at all). To the extent that the asset can be analysed under traditional conflict-of-laws rules as sited in the Cayman Islands, then a grant of representation would be required from the Cayman Islands court to preclude the risk of intermeddling claims in dealing with the asset in the Cayman Islands (even though the grant itself would not necessarily prevent someone with access to the private keys associated with a digital asset from dealing with the same).

The main potential difficulty that may arise is practical; namely that anyone inheriting a virtual asset will, on the face of it, often only be able to access that virtual asset if the personal representative of the deceased or the beneficiary (as the case may be) has or can obtain the information needed in order to gain access and control over that virtual asset (e.g. a private key to the wallet in which it is stored). Most exchanges have policies in place to transfer virtual assets to next of kin but these policies, and the transfer requirements, will vary across exchanges and it is generally regarded as prudent to avoid leaving significant value on exchanges for any length of time due to the risks of hacking and insolvencies.

* * *

Endnote

1. Known as the VASP Law until a recent change amending the way in which Cayman Islands primary legislation is referred to.

Chris Duncan
Tel: +1 345 749 2057 / Email: chris.duncan@careyolsen.com

Chris is in the corporate group of Carey Olsen and a partner of the firm. He advises on the full spectrum of digital assets, cryptocurrency and fintech matters across the Cayman Islands and the British Virgin Islands, from structuring and restructuring to regulatory matters and disputes, and is described by clients in *Chambers FinTech* as being "very familiar with the blockchain/Web3 space and developments in Cayman law". Chris also advises on a broad range of private client matters.

Chris was formerly with Mourant in Guernsey and a large firm in New Zealand. Chris obtained a Bachelor of Laws and a Bachelor of Science (majoring in Chemistry) from the University of Otago in New Zealand.

Alistair Russell
Tel: +1 345 749 2013 / Email: alistair.russell@careyolsen.com

Alistair is a partner in the corporate and finance group of Carey Olsen in the Cayman Islands and advises on all aspects of finance, fintech, corporate, investment funds and commercial law.

He has advised clients on a broad range of transactions including financing, fintech, ICOs, private equity, joint ventures, mergers and acquisitions and capital markets, and is described by clients in *IFLR1000* as "the best Cayman lawyer we've ever worked with".

Alistair was formerly with Skadden, Arps, Slate, Meagher & Flom and Cleary Gottlieb Steen & Hamilton, each in London.

Carey Olsen

PO Box 10008, Willow House, Cricket Square, Grand Cayman KY1-1001, Cayman Islands
Tel: +1 345 749 2000 / Fax: +1 345 749 2100 / URL: www.careyolsen.com

Cyprus

Akis Papakyriacou
Akis Papakyriacou LLC

Government attitude and definition

In February 2021, Directive (EU) 2018/843 of the European Parliament and of the Council of 30 May 2018 ("**AMLD5**") was transposed into Cyprus law through an amendment of the Prevention and Suppression of Money Laundering and Terrorist Financing Law 188(I)/2007 to 2019 (the "**AML Law**"). At the moment, the AML Law is the only legal framework in Cyprus that recognises and defines "Crypto-Assets". More specifically, the AML Law defines "Crypto-Assets" as being a digital representation of value that is not issued or guaranteed by a central bank or a public authority, is not necessarily attached to a legally established currency, does not possess a legal status of currency or money, is accepted by persons as a means of exchange or investment, and which can be transferred, stored, or traded electronically and is not:

(a) fiat currency;
(b) electronic money; or
(c) a "financial instrument" as this term is defined in Part III of the First Appendix of the Law that provides for the provision of investment services, the exercise of investment activities, the operation of regulated markets and other related matters, L.87(I)/2017.

In addition to the transposition of AMLD5 and the defining of "Crypto-Assets", we have seen the authorities and the regulator taking positive steps towards a more crypto-friendly approach. The Cyprus Securities and Exchange Commission (the "**CySEC**") has established an Innovation Hub, which aims to act as a platform for both supervised and non-supervised entities to come together and share knowledge in order to accelerate their business models in line with the CySEC's commitment to ensuring regulated entities' investor protection. The CySEC, via the Innovation Hub, offers support to market participants who are introducing innovative financial products or services. On 10 February 2020, the CySEC issued a "*Report on the Activities of CySEC's Innovation Hub*", which essentially describes the objectives of the Innovation Hub and outlines any progress made thus far. The CySEC notes that the Innovation Hub attracted full-spectrum interest from both Fintech and Regtech companies, supervised entities and entities not subject to supervision, from Cyprus and abroad.

The Cyprus government, by a Council of Ministers decision N.85.629 dated 30 August 2018, has formed an *ad hoc* working group to develop and implement blockchain technology in Cyprus. The priority in the national strategy is the enactment of a legal framework regulating blockchain and cryptocurrencies. Following the aforementioned decision N.85.629, three subcommittees of the working group were formed, namely: (a) a legal framework; (b) application in the public sector; and (c) application in the financial industry. The main objectives of the subcommittees are to (i) identify cases of public or private sector services that could be enhanced with Distributed Ledger Technology ("**DLT**"),

(ii) develop guidelines and specifications that should be taken into account in the future development of the National DLT Services Infrastructure for it to support the deployment of the identified public sector use cases, and (iii) identify the parameters that should be included in the proposed regulatory framework. The national strategy aims to regulate, through a legal framework, cryptocurrencies and the trading of cryptocurrencies, assuming a categorisation of cryptocurrencies into Security Tokens and Non-Security Tokens. For the sake of clarity, Security Tokens can be described as a new version of a financial instrument, allowing fractionalised ownership of different assets; they are essentially a digital analogue of a traditional security such as shares. At the moment, we do not have a universal definition for Security Tokens; however, Security Tokens that confer analogue rights to those conferred by shares arguably fall under the definition of "transferable securities" under Article 1(1)(44) of MiFID II, and more specifically under sub-section (c) providing that "*any other securities giving the right to acquire or sell any such transferable securities or giving rise to a cash settlement determined by reference to transferable securities, currencies, interest rates or yields, commodities or other indices or measures*" are deemed to be transferable securities.

On the other hand, Non-Security Tokens are unregulated tokens, which include Exchange Tokens and "cryptocurrencies" such as Bitcoin. These tokens utilise a DLT platform, and they are not backed or issued by a bank or other central body. They do not confer the rights conferred by Security Tokens but are instead used as means for investment or exchange.

It is apparent that Cyprus is taking important steps to keep up with the international developments and trends by introducing new and innovative technologies applicable to financial services.

Cryptocurrency regulation

The first step towards the regulation of cryptocurrencies was taken through the amendment of the AML Law, wherein "Crypto-Assets" have been defined, as per the first section, and further to this the AML Law now regulates the provision of services by Crypto-Asset Service Providers ("**CASPs**"). The AML Law defines a CASP as a person who provides or exercises one or more of the following services or activities to another person or on behalf of another person:

(a) Exchange between crypto-assets and fiat currencies.
(b) Exchange between crypto-assets.
(c) Management, transfer, holding, and/or safekeeping, including the custody of crypto-assets or cryptographic keys or means that allow the exercise of control over crypto-assets.
(d) Offering and/or sale of crypto-assets, including the initial offering.
(e) Participation and/or provision of financial services regarding the distribution, offer, and/or sale of crypto-assets, including the initial offering.

Financial services regarding the distribution, offer, and/or sale of crypto-assets are defined by the AML Law as the following investment services:

(a) Reception and transmission of orders.
(b) Execution of orders on behalf of clients.
(c) Dealing on own account.
(d) Portfolio management.
(e) Provision of investment advice.
(f) Underwriting and/or placing of crypto-assets on a firm commitment basis.
(g) Placing of crypto-assets without a firm commitment basis.
(h) Operation of a multilateral trading facility for buying and selling crypto-assets.

In this respect, any CASP that intends to offer any of the abovementioned services in Cyprus must register for anti-money laundering purposes at the CASP registry, which will be held by the CySEC.

The framework introduced through the AML Law is certainly a positive step forward for Cyprus becoming an attractive destination for investors and businesses engaging in crypto-asset-related activities; however, as this is still not a full regulatory framework, the concerns about the status and volatility of crypto-assets remain a key issue for the authorities. The Central Bank of Cyprus (the "**CBC**") and the CySEC, through the years prior to the transposition of AMLD5, had issued a number of warnings to potential cryptocurrency investors as well as to investment firms looking to deal in, promote or provide cryptocurrencies. A number of the concerns raised by these warnings are extinguished, at least partially, pursuant to the AML Law regulation of crypto-assets.

To be more precise, on 7 February 2014, the CBC issued an announcement with the title "*Attentions to the risks associated with virtual currencies*", whereby it highlighted that cryptocurrencies are not considered "*legal tender*", noting also that any activity relating to cryptocurrencies is not authorised by the CBC, stressing that "*the public needs to be aware of the fact that there are no specific regulatory measures to cover losses from the use of virtual currencies if the platform that exchanges or holds them collapses and thus there is the risk of losing the entire amount deposited*".

The CBC also sets out therein a non-exhaustive list of risks associated with cryptocurrencies, namely:

- There is a lack of guarantee or legal obligation to reimburse at face value.
- The price of virtual currencies is highly volatile; as a result, it may rise sharply or even fall to zero value.
- Any merchant may refuse to accept cryptocurrencies for payments.
- Transactions in cryptocurrencies are more likely to be misused for the purpose of illegal activities.

Along similar lines, the CySEC, on 6 February 2014, issued an announcement drawing the attention of the public, and particularly of potential investors, to the warning issued by the European Banking Authority regarding the risks in connection with, or arising out of, the purchase, possession or trading of cryptocurrencies. Furthermore, the CySEC shared the report on the characteristics, functions and risks of virtual currency as issued by the European Central Bank.

Following the aforementioned announcement, the CySEC, on 18 March 2014, issued an additional announcement outlining, *inter alia*, the following risks associated when buying, holding, exchanging, or trading in cryptocurrencies:

- Cryptocurrencies deposited in an e-wallet could potentially be stolen.
- Transactions in cryptocurrencies could potentially involve money laundering and terrorist financing activities.

The AML Law attempts to a great extent to eliminate the abovementioned issues associated with buying, holding, exchanging, or trading in cryptocurrencies, as it sets out certain parameters and requirements that a CASP must comply with in order to minimise and/or eliminate the risk of the above.

It is important to note than on 16 May 2023, the Regulation on Markets in Crypto-Assets ("**MiCA**") was adopted by the European Council and entered into force in June 2023. Therefore, we now have a uniform regulation within the EU, which is expected to be transposed into national law in 2024.

Sales regulation

Initial coin offerings ("**ICOs**") have become increasingly popular as a way of raising funds. It is very common for cryptocurrencies to be used in an ICO. There is no prohibition on ICOs in Cyprus, and since the amendment of the AML Law in February 2021, ICOs are regulated as they fall under the services provided by a CASP. In this respect, any person or entity wishing to perform an ICO must register with the CySEC as a CASP, subject to complying with all the requirements set by the CySEC for the registration, as summarised in the section "*Money transmission laws and anti-money laundering requirements*" herein.

Taxation

Any funds that derive from an ICO are subject to tax in Cyprus as they are deemed to be taxable income; however, Cyprus has one of the lowest and most attractive corporate tax rates at 12.5%. With respect to the value-added tax ("**VAT**") treatment of ICOs, it is noted that, at the moment, the guidance with respect to the VAT treatment of cryptocurrencies is limited, and most of it comes from the European Court of Justice judgment of case C-264/14 *Hedqvist*, which provided the basis for the VAT treatment of transactions concerning the exchange of traditional currencies for Bitcoins and *vice versa*, noting that these are exempt from VAT. On the matter of Security Tokens, based on their function these may be deemed to be equity or debt liability and may therefore be excluded from both corporate tax and VAT.

Money transmission laws and anti-money laundering requirements

On 25 June 2021, the CySEC issued the Directive for the registration of CASPs (the "**Directive**") pursuant to the AML Law.

As discussed in the previous sections, the AML Law provided a long-awaited definition for CASPs and was the first step towards the regulation of crypto-asset-related activities, providing that any provider carrying out activities relating to crypto-assets must register in the relevant CySEC registry (the "**Registry**") as a CASP.

CASP registration

The Registry is publicly available on the CySEC's website, and it has the following information for each CASP:

(1) Name, tradename, legal form and company registration number of the CASP.
(2) Physical address of the CASP.
(3) Services offered and/or activities performed, pursuant to the services set out in the CASP definition in the law.
(4) The CASP's website.

At the time of writing, nine companies have been registered as CASPs in the Registry, while another 10 companies registered in other Member States have been registered in the EEA CASP Register.

CASP registration requirements

The CySEC approves the applicant's registration as a CASP provided that the applicant complies with the following:

(1) The applicant must have submitted all information, documents and data required in the application form (which will be published by the CySEC in due course) and/or which may be requested by the CySEC during the review of the application, and especially the applicant must also provide the information set out in the previous section, as well as the addresses of all crypto-assets.

(2) The applicant must ensure that members of the Board and anyone in a managerial position are honest and capable, which is satisfied by showing good repute, knowledge, skills and expertise, and by dedicating adequate time to the performance of their duties.
(3) The Board of Directors of the applicant must have at least four members, who satisfy the provisions of point (2) above, out of which at least two must be executive members and the other two must be independent, non-executive members.
(4) The applicant must ensure that its beneficial owners are honest and competent, something that may be satisfied by evidencing good repute and skills to maintain the good financial structure of the applicant.
(5) In the event that the applicant will be operating online, it must maintain its exclusive website, through which it will be operating, without giving access to any other person to operate through this website.
(6) The applicant must have established proper policies and procedures that ensure its compliance, including compliance by its members, employees and assignees, with the AML Law and the Directive.
(7) The applicant must have established proper policies and procedures and have in place appropriate systems and control mechanisms in order to ensure its prudent operation, including minimisation of the risk of appropriation or loss of its clients' crypto-assets.
(8) Capital requirement compliance – the applicant must maintain, at all times, own funds equal to the higher of the following amounts:
    (a) (i) EUR 50,000 initial capital for the provision of investment advice with respect to crypto-assets. (ii) EUR 125,000 initial capital for the provision of the following services: reception and transmission of orders; execution of orders on behalf of clients; exchange between crypto-assets and fiat currencies; exchange between crypto-assets; participation and/or provision of financial services regarding the distribution, offer, and/or sale of crypto-assets, including the initial offering; placing of crypto-assets with a firm commitment basis; and portfolio management. (iii) EUR 150,000 initial capital for the provision of the following services: management, transfer, holding, and/or safekeeping, including the custody of crypto-assets or cryptographic keys or means that allow the exercise of control on crypto-assets; placing of crypto-assets without a firm commitment basis; and operation of a multilateral trading facility for buying and selling crypto-assets.
    (b) One-quarter of the applicant's fixed expenses on the basis of the previous year, to be revised annually. This will be calculated pursuant to the provisions of the Directive.
(9) The applicant must ensure that remuneration terms of the staff are such that they do not conflict with the staff's duty to act in the best interests of the clients, and that the applicant does not make any adjustments in remuneration, targets of sales or otherwise that could act as a motivation for the staff to implement aggressive marketing techniques.
(10) The applicant must have established proper arrangements of corporate governance with transparent and clear reference lines.
(11) The applicant must take all reasonable measures to ensure the continuing operation of its activities and have in place proper and up-to-date policies for ensuring its continuing operations and proper and up-to-date policies and procedures for the retrieval of data and timely continuance of operations where, despite the reasonable measures in place, its operations have ceased.
(12) The applicant must arrange for the outsourcing of essential functions, in order for reasonable measures to be taken to avoid any undue deterioration of the operational risk.

(13) The applicant must have established proper administrative and accounting procedures, internal control mechanisms, effective procedures for risk assessment and effective security and control mechanisms in place for its electronic data processing systems.
(14) Where the scope, nature, scale and complexity of the activities require, the applicant must establish an internal control function that is independent from the other functions and operations of the applicant.
(15) The applicant must have established proper security mechanisms, for the purpose of ensuring and verifying the authenticity of the means used for transmission of information, for the minimisation of the risk of destruction of data and of the risk of non-authorised access, as well as prevention of any information leakages, in order to ensure that confidentiality is maintained at all times.
(16) The applicant must ensure that records are kept with respect to all its activities, which also includes relevant communications, and such records must be kept in such a manner as to enable the CySEC to perform its duties and to take such steps as to ensure the applicant's compliance with its obligations.
(17) The applicant must ensure that its staff are not involved in multiple duties and, if they are, the applicant must ensure that this does not affect or may not affect such staff from performing any of their duties diligently, professionally and with honesty.
(18) The applicant must establish proper policies and procedures in order to ensure that any complaints from clients are duly addressed.
(19) The applicant must ensure that its staff are honest and professional and have the required knowledge on the basis of their duties.

Removal from the Registry

The CySEC may remove a CASP from the Registry if any of the following applies:
(a) The CASP has ceased offering services relating to crypto-assets for a period of six months.
(b) The CASP has been registered pursuant to false representations or in any other irregular manner.
(c) The CASP has ceased all services and activities that fall under the definition of CASP pursuant to the law.
(d) It no longer falls under the provisions of the law.

Applicable fees

(1) The applicant pays a fee of EUR 10,000 together with its application for registration as a CASP. This amount is not refundable in the event that the applicant is rejected. In the event that the applicant is registered as a CASP, then there is no other fee or contribution payable to the CySEC for the first year of its registration.
(2) Each year after the registration there is a renewal fee of EUR 5,000 payable to the CySEC.
(3) In order to notify the CySEC of a substantial alteration, the following fees are applicable:
    (a) EUR 1,000 per activity or service.
    (b) EUR 2,000 per notice of change relating to the members of the Board of Directors of the CASP.
    (c) EUR 5,000 per notice of change relating to the beneficiaries of the CASP.
    (d) EUR 1,000 per notice of change relating to the website of the CASP.

The CySEC supplemented the provisions of the AML Law and of the Directive with the introduction of the Policy Statement on the Registration and Operations of CASPs, which was issued on 13 September 2021. The Policy Statement clarified a number of matters, such as the overlapping between certain activities, stressing that activities requiring registration as a CASP under the AML Law refer to the end result, which, in the CySEC's view, describe an end result, which may be achieved through a combination of other services and/or activities.

Additionally, in its Policy Statement, the CySEC highlights that the implementation of the "Travel Rule" is rendered necessary under the requirement of applying a risk-based approach, which is the obligation to obtain, hold, and transmit originator and beneficiary information in order to identify and report suspicious transactions, monitor the availability of information, take freezing actions, and prohibit transactions where appropriate.

Promotion and testing

The CySEC has established an Innovation Hub to foster a better, more effective relationship between entities operating, *inter alia*, in the areas of cryptocurrencies and blockchain. Further to the CySEC's initiative to set up the Innovation Hub, the Cyprus government has also taken the first steps towards the implementation of blockchain technology in Cyprus, through the formation of an *ad hoc* working group. A more extensive account of the objectives and actions of the Innovation Hub and of the *ad hoc* working group is given in the "*Government attitude and definition*" section above.

Ownership and licensing requirements

As per the previous sections, all entities intending to offer services falling under the definition of a CASP pursuant to the AML Law must register in the Registry in order to be able to perform their activities as CASPs. Other than the AML Law, there is currently no other specific restriction and/or licensing requirement under Cyprus law.

Mining

Currently, there is no specific restriction and/or licensing requirement under Cyprus law.

Border restrictions and declaration

Currently, there is no specific restriction under Cyprus law.

Reporting requirements

Reporting requirements apply only to derivatives on cryptocurrencies.

Estate planning testamentary succession

At the moment, there is no legal framework, regulation and/or guidance as to how testamentary succession of cryptocurrencies should be treated. We have therefore made the assumption that the treatment of cryptocurrencies would be the same as the treatment of any other movable property in Cyprus.

Subject to the provisions of EU Regulation 650/2012, the Wills and Succession Law Cap 195 regulates wills and intestacy; it applies to the estate of any deceased person with a Cyprus domicile, and to all immovable property located in Cyprus. That is, Cyprus succession laws will apply to movable and immovable property of a person domiciled in Cyprus, and to Cyprus-*situs* immovable property irrespective of the deceased's domicile at the time of death. It is noted that it is not obligatory for a will to be made and, in the absence of a will, the property is distributed on the basis of Cyprus succession laws.

It should be noted that even where there is a will, there are restrictions with respect to the manner in which property can be disposed of. Cyprus succession laws implement a forced heirship regime, which means that certain relatives, such as a spouse or children, cannot

be excluded from an inheritance and they have a right to a fixed minimum percentage of the estate. It should be noted that the forced heirship regime applies to everyone who dies domiciled in Cyprus, regardless of nationality; however, EU citizens are conferred the rights by EU Regulation 650/2012 to choose the law of their country of nationality as the law applicable to their estate; in such case, it should be expressly provided for in the will. Where the deceased leaves no spouse, child or descendant of a child, the rules of forced heirship do not apply and 100% of the estate of the deceased who is domiciled in Cyprus may be disposed of freely by will.

The above description of Cyprus succession laws is made on the assumption that the treatment of the succession of cryptocurrencies will be the same as for movable property in Cyprus. We have no other indication thus far as to how the succession of cryptocurrencies will be treated once a legal framework is formed.

Akis Papakyriacou
Tel: +357 22 256 882 / Email: akis@papakyriacoulaw.com

Akis graduated from the University of Salford with first-class honours (LL.B.) and obtained his M.Sc. from the University of Oxford (Corpus Christi). Akis attended the City Law School where he passed the Bar Professional Training Course (Very Competent). Following the completion of his studies, Akis returned to Cyprus to complete his vocational training in one of the leading law firms, where he continued working after the completion of his training, specialising in corporate, banking and finance law until September 2018. Prior to forming Akis Papakyriacou LLC, Akis worked as a partner in a law firm in Nicosia.

Akis focuses on corporate, banking and finance transactions, with experience in both local and international finance transactions. His knowledge and expertise also extend to merger and acquisition transactions, corporate restructurings, employment law matters and fund-related matters.

Akis Papakyriacou LLC

20 Stasikratous Street, 2nd Floor, Office 203, 1065, Nicosia, Cyprus
Tel: +357 22 256 882 / URL: www.papakyriacoulaw.com

France

Hubert de Vauplane, Victor Charpiat & Morgane Fournel Reicher
Kramer Levin Naftalis & Frankel LLP

Government attitude and definition

The government seems to be supporting blockchain-based technologies in general.

France has become the central European hub for crypto and blockchain companies and several French start-ups have begun their international expansion. The following are examples of business models developed by French start-ups:

- exchange platforms for retail investors (Paymium);
- digital asset brokers such as Coinhouse, Meria and Deskoin, enabling investors to trade digital assets directly with legal currency without using an exchange platform;
- prime brokers offering over-the-counter ("OTC") services to institutional services, such as Woorton and Aplo;
- hardware wallet manufacturers such as Ledger (arguably the most prominent French blockchain company);
- data collection and analytics services such as Kaiko, offering market data on digital asset exchanges to institutional clients;
- blockchain software development companies, including Nomadic Labs and ARK.io;
- layer 1 blockchain solutions such as Massa Labs, a company developing a high-performance, scalable blockchain infrastructure;
- consulting and outsourced project management firms, such as Blockchain Partner, as well as numerous other smaller players in the market;
- decentralised finance ("DeFi") platforms, such as Morpho, Angle, Paladin, ParaSwap, Mangrove and Kleros; and
- digital asset tax reporting and compliance tools (Waltio).

This dynamism is mostly due to the adoption in 2019 of a dedicated legislation designed to allow France to become a leading jurisdiction for blockchain technology: the PACTE Act, which stands for "Action Plan for the Growth and Transformation of Companies". This legislation introduced the first comprehensive regulatory framework in France for initial coin offerings ("ICOs") and intermediaries dealing with cryptocurrencies (digital asset service providers, or "DASPs").

Consequently, at the time of writing, 96 companies are registered as DASPs, and one is licensed under this statute.

Cryptocurrency regulation

France's desire to become a major European crypto hub was made clear by its adoption on May 22, 2019 of the PACTE Act.[1] The PACTE Act established a clear regulatory framework applicable to DASPs and ICOs. Under the PACTE Act's regulatory framework, a DASP is

required to register with the Financial Markets Authority (*Autorité des Marchés Financiers*, or "AMF") when it provides at least one of the following four services: (1) custody of digital assets on behalf of third parties; (2) buying or selling digital assets in legal currency; (3) exchanging of digital assets for other digital assets; and (4) operation of a digital asset trading platform.

The illegal practice of any of the above-mentioned activities without appropriate, prior registration is punishable by two years' imprisonment and a fine of EUR 30,000, pursuant to Articles L.54-10-2 and L.572-23 of the French Monetary and Financial Code ("CMF").[2]

Relatedly, assets that incorporate features and/or rights that pertain to financial instruments or electronic money are qualified as such and therefore excluded from the digital asset legal category. Such assets can only be issued and traded in accordance with regulations deriving from applicable regulations, and follow the appropriate regime.

DASP regulation

The actual statutes: Reinforced registration and the licence

Recently, this regulatory framework has been strengthened by the reinforcement of the supervisory and enforcement powers of the AMF: the regulator will be able to take precautionary measures when it considers that a DASP is susceptible to becoming insolvent, and may further suspend the registration of a DASP where its activity is deemed a threat to the stability of the digital asset market.

Secondly, a new registration statute has been introduced, which will become mandatory as of January 1, 2024. Since July 1, 2023, companies have been required to register under the reinforced registration statute. The AMF has continued to register DASPs under the prior regime in cases where such DASPs had submitted a complete application before July 1, 2023.

DASP registrations are processed and instructed by the regulators once the registration file has been submitted to the AMF. The application must include all the documents specified in Article D.54-10-2 of the CMF.[3]

Under the reinforced registration regime, companies are required to ensure the following:

- compliance with anti-money laundering and counter-financing of terrorism ("AML/CFT") regulations;
- establishing of a resilient and secure IT infrastructure, adopting a detailed cybersecurity policy, and submitting an audit report from a certified cybersecurity consultant (which shall be based in France);
- implementation of adequate security and internal control systems;
- adoption and implementation of additional procedures related to conflicts of interest, complaints handling, internal controls, incident reporting, outsourcing, as well as publishing of a pricing policy, etc.;
- depending on the services actually provided, adoption of dedicated policies. This could result in establishing, in particular, a detailed custody policy and guarantees that the DASP's own assets are segregated from its users' assets;
- inclusion of mandatory information and disclaimers in the T&Cs and marketing content, and communicating clear, accurate and non-misleading information to their clients; and
- in addition, the regulator will have expectations in relation to the "substance" of the entity, i.e., its staffing. Notably, the AMF usually expects the executive manager(s) of the entity to be based in France.

Optionally, a licence can be obtained for DASPs that are already registered, and/or for services that only require optional registration. Only one company has been licensed so far, which is Société Générale Forge.

The licence application is substantially similar to that for reinforced registration, except for capital requirements.

The requirements of the DASP licence regime are substantially similar to the statute that will be required once the Markets in Crypto-Assets Regulation ("MiCA") has come into application (the crypto-asset service provider ("CASP") statute). As a result, obtaining a DASP licence can accelerate and facilitate the process of obtaining a CASP statute and the associated passport.

The main reasons for applying for an optional DASP licence are:
- Using the licence as a marketing and canvassing tool to gain market share.
- Anticipating the introduction of the new CASP licence under MiCA.
- Sponsoring sports/e-sports teams and events, as only licensed DASPs are legally allowed to do so.
- MiCA was adopted on April 23, 2023 by the European Parliament. This text provides a clear and harmonised European framework for the regulation of the issuance and provision of services related to crypto-assets and stablecoins. The EU has become the first major jurisdiction to do so.

Prospective regulations

Under MiCA, all CASPs active on the European market will be obliged to apply for a CASP licence. They will benefit from an 18-month transition period, ending in July 2026, to comply with the new MiCA requirements. During this period, registered or licensed DASPs from an EU Member State's statute can validly continue to offer their services, but without the European passport.

Under MiCA, CASPs will be required to comply with the following requirements:
- AML/CFT compliance;
- own funds requirements;
- compliance with the Digital Operational Resilience Act ("DORA"): Establishing a resilient and secure IT infrastructure, adopting a detailed cybersecurity policy, and submitting an audit report from a certified cybersecurity consultant (which shall be based in France);
- adoption and implementation of market abuse procedures;
- compliance with requirements in terms of sustainability of the digital assets held/managed;
- implementation of adequate security and internal control systems;
- adoption and implementation of additional procedures related to conflicts of interest, complaints handling, internal controls, incident reporting, outsourcing, as well as publishing of a pricing policy, etc.;
- depending on the services actually provided, adoption of dedicated policies. This could result in establishing, in particular, a detailed custody policy and guarantees that the CASP's own assets are segregated from its users' assets;
- inclusion of mandatory information and disclaimers in the T&Cs and marketing content, and communicating clear, accurate and non-misleading information to their clients; and
- in addition, the regulator will have expectations in relation to the "substance" of the entity, i.e., its staffing. The AMF expects the executive manager(s) of the entity to be based in France.

Stablecoin issuers will be required to be licensed as either electronic money institutions, credit institutions, or providers licensed under MiCA, depending on the qualification of the stablecoin to be issued.

In addition, the following regulations or regimes are expected to come into force in the following months/years:

- The Distributed Ledger Technology ("DLT") Pilot Regime ("Pilot Regime"), part of the Digital Finance Package alongside MiCA, which was adopted in June 2022.[4] The Pilot Regime is intended to develop a regulatory framework for trading and settlement for DLT's financial instrument.
- The revised Transfer of Funds Regulation (EU) 2015/847 on information accompanying transfers of funds ("TFR"), which was adopted on April 20, 2023. TFR aims to strengthen the EU's AML/CFT rules by transposing the Financial Action Task Force's ("FATF") Travel Rule requirements into EU law. TFR therefore establishes a dedicated framework for tracing the transfers of crypto-assets by imposing Travel Rule requirements on CASPs. Accordingly, EU CASPs will be required to comply with the Travel Rule obligations for every transaction, regardless of amount. No *de minimis* threshold will apply, and there will be no simplification of requirements for transactions within the EU. Stronger requirements will apply to transactions with self-hosted wallets. TFR will apply from January 2025 (18 months after the regulation enters into force).
- At a French level, on March 9, 2023, Law 2023-171 ("DDADUE Law")[5] defined the assignment of responsibilities of the respective national authorities, which apply exemptions according to the Pilot Regime.

ICOs

The public offering of tokens is defined as a fundraising operation using DLT, which gives rise to an issue of tokens (Article L.552-3 CMF).[6]

Article 85 of the PACTE Act allows issuers to apply for an optional visa from the AMF, which indicates that the "information document" for this contemplated ICO has been validated by the regulator and deemed satisfactory regarding the information disclosed to the potential investors (Article L.552-4 CMF).[7] This visa, which a company may or may not request, gives issuers access to a wider range of communication methods. The visa extends the scope of potential commercial communications to solicitation, sponsorship and patronage.

The visa must be issued prior to the public offering and when applying for a visa, the issuer must meet certain conditions, as follows:

- The legal entity must be established or registered in France.
- The white paper must comply with the requirements set out in Article 712-1 of the General Regulations of the AMF ("RG AMF") and the AMF instruction DOC-2019-06 of June 6, 2019 (concise and comprehensible to subscribers, so that investors understand the risks).
- Implementation of a procedure for monitoring and safeguarding collected assets (Article 712-7 RG AMF and the AMF instruction mentioned above).
- Implementation of a system to combat money laundering and the financing of terrorism.

The project must be accompanied by the following documents, which must be up to date, signed and in French or English:

- A draft information document in compliance with Articles 712-2 to 712-5 of the RG AMF.[8]
- An up-to-date copy of the articles of association.
- An up-to-date copy of the Kbis extract from the Trade and Companies Register.
- The balance sheet and income statement for the last financial year.
- An extract from the corporate officer's criminal records within the meaning of Article L.225-185 of the French Commercial Code.
- Any document justifying the implementation of a system for monitoring and safeguarding the assets collected in connection with the offering.

- Any document justifying the implementation of systems enabling the token issuer to comply with its AML obligations.
- All promotional communications relating to the offer.
- Legal documentation relating to the token issuing.

Following the above, the AMF examines the whole project. The authority has 20 business days to notify its decision to grant the visa. Any refusal must be duly justified by the regulator.

This regime must be distinguished from the security token offering ("STO"). The PACTE Act and the AMF, with its publication and guidelines, have clarified that tokens that are deemed financial instruments are not eligible to the ICO regime and should be issued as part of an STO.

Sales regulation

The concepts of securities and commodities do not exist under French law. The CMF qualifies Bitcoin and other cryptocurrencies as digital assets within the meaning of French law and classifies them under two categories, pursuant to Article L.54-10-1 of the CMF:

- Tokens that represent one or several rights that can be issued, registered, retained or transferred by means of a distributed database enabling the owner of the asset to be identified. In accordance with Article L.553-2 of the CMF, financial instruments (Article L.211-1 CMF) and cash vouchers (Article L.223-1 CMF) are excluded.
- Digital currencies refer to any digital representation of value that is not issued or guaranteed by a central bank, is not necessarily attached to legal tender and does not have the legal status of a currency, but which is accepted as a medium of exchange and can be transferred, stored or exchanged electronically.

Taxation

Income tax

The tax regime applicable to capital gains on the sale of digital assets depends on the investor's applicable tax statute. A new tax regime came into force on January 1, 2023, which is based on the distinction between individual and professional sellers.

Primarily, a taxable event would occur whenever a digital asset transfer is realised in return for a good, a service or legal tender.

Thus, the individual investor will be taxed at a flat rate of 30% of the total sum of capital gains deducted from all capital losses realised by members of the tax household. However, individual investors can opt to have their capital gains taxed in another tax category, the industrial and commercial profits category ("BNC"). The taxable event is the transfer for consideration of a digital asset for any counterparty other than a digital asset. Unrealised gains on cryptocurrencies circulating within decentralised services are therefore not subject to tax[9] (Article 150 VH *bis* of the French General Tax Code, or "CGI").

Professional investors will be subject to the progressive tax scale in the BNC category, with no option to opt for flat-rate taxation. The marginal rate of income tax and social security contributions can reach 60% of taxation. This system also applies to crypto-asset miners (Article 92 CGI).

Companies

According to the accounting standards issued by the French Accounting Standards Authority ("ANC"), tokens that qualify as financial instruments will be accounted for as such. Other tokens will be accounted for according to the rights and obligations attached. Digital assets are registered under a dedicated account and specific rules.

Capital gains and losses on tokens held should be calculated at the time of sale, as detailed in the previous section.

VAT

The sale of a good or service in cryptocurrency is treated as a means of payment similar to those executed with any other means of payment. The provisions relating to the sale must be complied with, including the VAT rate to be paid to the tax authorities.

Transactions involving the exchange of cryptocurrencies with traditional currencies, as well as transactions between these digital assets, are exempt from VAT according Article 261 C of the CGI and the European Union Court of Justice ruling of October 22, 2015 (*Hedvist*).[10]

The tax authorities clarify that this is the case because the principle of future benefits is uncertain. For a transaction to be subject to VAT, there must be a direct link between the service provided and the benefit received. This is why mining is not subject to VAT. As miners are only remunerated when they win the validation of a block, remuneration has a random nature. As such, there is no individualised service provided by the miner for a specific beneficiary. The miner does not have to collect VAT on digital assets received as a reward.

Money transmission laws and anti-money laundering requirements

In France, money laundering is an infraction punishable by five years' imprisonment and a EUR 375,000 fine under Article 324-1 of the Criminal Code.[11] Financing of terrorism is an infraction punishable by 10 years' imprisonment and a fine of EUR 225,000 under Article 421-5 of the Criminal Code.[12]

The following entities providing services or offerings on digital assets are required to comply with AML/CFT regulations:

- DASPs that are required to register with the AMF (i.e., entities providing the service(s) of (i) custody of digital assets, (ii) buying or selling digital assets in legal tender, (iii) trading of digital assets for other digital assets, and (iv) the operation of a trading platform for digital assets).
- DASPs providing other services related to digital assets that choose to apply for a DASP licence with the AMF.
- ICOs whose issuance has been approved by the AMF by means of a visa, but only with respect to the subscriptions received pursuant to the ICO.
- Other actors (i.e., mostly DASPs that do not provide custody, crypto-fiat or crypto-crypto brokering services and the operation of a digital asset trading platform) are not subject to any AML obligations, provided the services they provide do not fall within the scope of AML/CFT legislation.

In accordance with the applicable AML directives and the DASP regime, registered DASPs are required to identify, assess and classify the risks to which they are exposed with respect to the activity they carry out, in order to provide effective guarantees that their services are provided in compliance with applicable AML/CFT regulations. This includes establishing and enforcing risk classification procedures in accordance with Article L.561-4-1 of the CMF.

The AMF and the Prudential Supervision Authority ("ACPR") are responsible for assessing, prior to granting a statute or visa, and on a continued basis once the relevant statute has been granted, the effectiveness of the AML/CFT procedures implemented by the companies subject to this regulation.

In September 2022, for the first time, the AMF decided to sanction a DASP by withdrawing its registration due to non-compliance with the AML/CFT requirements.[13] This withdrawal followed an on-site inspection by the ACPR.

AML Package

In parallel, new EU measures against AML/CFT are in the process of being adopted. This package includes three pieces of draft legislation on the financing provisions of EU AML/CFT policy and consists of:

- The creation of a new European AML/CFT authority ("AMLA"). This authority will have supervisory, investigative and sanctioning powers regarding European financial institutions.
- A regulation entitled the EU "single rulebook" or "AMLR". This regulation includes guidelines that complete and standardise the regime for several concepts, notably customer due diligence and the use of crypto-assets.
- The sixth Anti-Money Laundering Directive. This text extends the scope of the previous directive and strengthens cooperation between financial intelligence units.
- A revision of the 2015 TFR, which makes the FATF's Travel Rule applicable to crypto-assets.

DeFi protocols should not be subject to these new measures. However, this is contingent on the protocol being deemed sufficiently decentralised, hence not being subject to the applicable and prospective DASP regulation.

Promotion and testing

At the date of this publication, France does not provide for a regulatory sandbox dedicated to blockchain or fintech initiatives, and there are no immediate plans by French regulatory authorities to implement a national regulatory sandbox.

By contrast, the European Commission launched a blockchain regulatory sandbox in February 2023. This project establishes a pan-European framework for regulatory dialogues in cases involving DLT and aims to increase the legal certainty for innovative projects of this ecosystem. The selection involves 20 solutions of different industry sectors and geographic regions. The selection process is realised by a panel of independent academic experts.

Further, the Pilot Regime enables licensed investment service providers to issue, register, transfer or store financial instruments using a distributed ledger, within a regulatory framework that guarantees investor protection, market integrity and financial stability.

Ownership and licensing requirements

Asset managers may not manage funds or mandates invested in both traditional financial instruments and crypto-assets, or exclusively in crypto-assets. In addition, it is currently impossible to combine the services of regulated asset management companies and DASPs.

However, the PACTE Act has granted some categories of investment funds the ability to invest in digital assets, as defined under Article L.54-10-1 of the CMF. This is made possible for specialised professional funds, provided they comply with the applicable liquidity and valuation rules, and for professional private equity funds, up to a limit of 20% of their assets.

To date, the following asset managers have developed digital asset offerings:

- In 2017, TOBAM launched a specialised professional fund fully invested in physically held Bitcoin. In October 2021, it became the first investment fund to be licensed by the AMF. The investment fund, TOBAM BTC Equity, which is eligible to invest in insurance products, has developed a strategy that combines Bitcoin with other assets. Further, the fund invests in a basket of actions in companies operating in the crypto-asset sector, or that own crypto-assets in their respective balance sheet, and whose aggregate value replicates the price of Bitcoin.

- Arquant Capital was licensed in 2022 for the commercialisation of investment funds dedicated to digital assets, including active management of a fund fully invested in digital assets.
- ExoAlpha is an investment firm that focuses its investment strategy on futures on digital assets, and has developed a particular strategy on emerging markets and commodities.
- CoinShares has developed two segments of activity:
  - CoinShares Asset Management, which offers exchange-traded products that are exposed to digital assets to institutional and professional investors; and
  - CoinShares Software, which provides for trading software on digital assets.

Mining

Mining is authorised in France. Indeed, this activity is not subject to any particular regulation. However, in practice, very few companies mine cryptocurrencies in France. Nevertheless, some companies, such as Summit Mining, are offering services whereby investors can purchase a share of a mining field and perceive some of the assets that are generated as a result of the mining activity. These kinds of service allow people with little computing capacity to participate in a collaborative way to mining activities.

Border restrictions and declaration

Under French tax law, there is an obligation to declare digital asset accounts opened, held, used or closed abroad, in accordance with Article 1649 *bis* C of the CGI.[14] However, there is no requirement to declare crypto-assets when entering or leaving French territory.

Reporting requirements

There are no reporting obligations other than those relating to AML/CFT. In the event suspicious activity, a DASP is obliged to report the transaction to TracFin.[15] In case of significant risk, DASPs are required to freeze assets and file a report to TracFin. It is not an automatic reporting system but is based on objective criteria defined *ex ante*. The analysis has to be carried out case by case by the entity. The due diligence obligation is determined according to a risk-based approach. Analysis of suspicious transactions must be pragmatic and supported by an internal system for detecting anomalies.

TFR, as part of the AML Package, which will apply to CASPs from December 2024, provides for enhanced traceability of crypto-asset transfers and identity verification (know-your-customer, or "KYC"). The newly adopted regulation consists of an amendment to the 2015 TFR regulation, which transposes the FATF's Travel Rule under EU law.

TFR aims to strengthen the EU's AML/CFT rules by transposing the FATF's Travel Rule requirements into EU law. TFR therefore establishes a dedicated framework for tracing crypto-asset transfers by imposing Travel Rule requirements on CASPs. Accordingly, as detailed above, EU CASPs will be required to comply with Travel Rule obligations for every transaction, regardless of amount. No *de minimis* threshold will apply, and there will be no simplification of requirements for transactions within the EU. Stronger requirements will apply to transactions with self-hosted wallets, according to which transfers of more than EUR 1,000 between a CASP and a self-hosted wallet will be subject to the appropriate reporting requirements. TFR will apply from January 2025 (18 months after the regulation enters into force).

Information will have to be collected, stored and transmitted in compliance with the General Data Protection Regulation.

Estate planning and testamentary succession

Crypto-assets are immaterial movable property under French law. As such, crypto-assets should be included in the estate declaration without benefitting from any special regime.

However, public officers are becoming increasingly aware of these new testamentary practices, and some are offering to collect shards of the private keys in order to ensure their transmission.

* * *

Endnotes

1. Law n° 2019-486 of May 22, 2019, Articles 85 to 88: https://www.legifrance.gouv.fr/jorf/id/JORFTEXT000038496102
2. Article L.572-23 of the CMF: https://www.legifrance.gouv.fr/codes/article_lc/LEGIARTI000038509771
3. Article D.54-10-2 of the CMF: https://www.legifrance.gouv.fr/codes/article_lc/LEGIARTI000043382030
4. Pilot Regime n° 2022/858: https://eur-lex.europa.eu/legal-content/FR/TXT/?uri=CELEX%3A32022R0858
5. DDADUE Law: https://www.legifrance.gouv.fr/jorf/id/JORFTEXT000047281777
6. Article L.552-3 of the CMF: https://www.legifrance.gouv.fr/codes/article_lc/LEGIARTI000038509547
7. Article L.552-4 of the CMF: https://www.legifrance.gouv.fr/codes/article_lc/LEGIARTI000038509549/2023-09-29
8. Article 712-2 of the General Regulation: https://www.amf-france.org/fr/eli/fr/aai/amf/rg/article/712-2/20190605/notes
9. Article 150 VH *bis* of the CGI: Article 150 VH *bis – Code général des impôts* – Légifrance: https://www.legifrance.gouv.fr/codes/article_lc/LEGIARTI000038612228
10. *Hedvist* ruling: EUR-Lex – 62014CJ0264 – EN – EUR-Lex: https://www.legifrance.gouv.fr/codes/article_lc/LEGIARTI000038612228
11. Article 324-1 of the Criminal Code: https://www.legifrance.gouv.fr/codes/article_lc/LEGIARTI000006418331
12. Article 421-5 of the Criminal Code: https://www.legifrance.gouv.fr/codes/article_lc/LEGIARTI000032925381
13. The withdrawal of a DASP registration: https://www.amf-france.org/fr/actualites-publications/communiques/communiques-de-lamf/lamf-et-lacpr-annoncent-la-radiation-du-psan-bykep-sas
14. Article 1649 *bis* C of the General Tax Code: https://www.legifrance.gouv.fr/codes/article_lc/LEGIARTI000037988279
15. Article L.561-15 of the CMF: https://www.legifrance.gouv.fr/codes/article_lc/LEGIARTI000033517847

Hubert de Vauplane
Tel: +33 1 44 09 46 80 / Email: hdevauplane@kramerlevin.com
Hubert de Vauplane is the co-head of Kramer Levin Naftalis & Frankel LLP's alternative investment management and fintech practices. He advises under EU and French laws on banking and investment services regulatory matters, asset management and funds, and financial/securities litigation, e-money and payment services, digital asset services, and derivatives products. Hubert advises corporates, asset managers, corporates, investment banks, and institutional investors on the entire range of disintermediated financings, including the structuring of debt funds. He is also a professor at the Paris Institute of Political Sciences (IEP Paris).

Victor Charpiat
Tel: +33 1 44 09 46 69 / Email: vcharpiat@kramerlevin.com
Victor Charpiat's practice focuses on banking and financial regulation, as well as the regulation of fintech and crypto-assets. He advises French and foreign digital asset service providers, investment firms, payment institutions and e-money institutions on the regulatory aspects of their activities.

Morgane Fournel Reicher
Tel: +33 1 44 09 46 67 / Email: mfournelreicher@kramerlevin.com
Morgane Fournel Reicher's practice focuses on financial market regulations, as well as the regulation of fintech, blockchain and cryptocurrencies. Morgane also advises French and foreign financial institutions with respect to financial services, notably alternative financial investments.

Kramer Levin Naftalis & Frankel LLP

47 avenue Hoche, 75008 Paris, France
Tel: +33 1 44 09 46 00 / URL: www.kramerlevin.com

Gibraltar

Jay Gomez, Javi Triay & Johnluis Pitto
Triay Lawyers Limited

Government attitude and definition

Gibraltar has a positive and welcoming attitude towards cryptocurrencies and blockchain technology. Gibraltar has been proactive in creating a favourable regulatory environment for crypto-related businesses. This is illustrated by the enactment of the Financial Services (Distributed Ledger Technology) Regulations ("DLT Regs"). Gibraltar became the first jurisdiction to provide a clear and comprehensive regulatory framework for blockchain and cryptocurrency businesses. The framework provided regulatory certainty when none could be found and seeks to ensure consumer protection and protect market integrity and financial stability without inhibiting innovation, thereby making it an attractive destination for companies operating in the blockchain and digital currency space.

The Gibraltar Financial Services Commission ("GFSC") regulates distributed ledger technology providers ("DLT Firms"), which include cryptocurrency exchanges and wallet providers. Firms operating within this space are also required to comply with anti-money laundering ("AML") and counter-terrorist financing ("CFT") regulations, as well with the Proceeds of Crime Act 2015 ("POCA").

By establishing a clear regulatory framework, Gibraltar has signalled its commitment to the space and to fostering a secure, well-regulated environment for DLT Firms to operate in. This approach has attracted various blockchain companies to set up operations in Gibraltar, which, in turn, has boosted the territory's economy and technological development.

It should be noted that cryptocurrencies themselves are not regulated. The Government has sought fit to regulate access points to the markets as opposed to regulating cryptocurrency, specifically. This approach has been welcomed by the industry.

While the Government has taken a positive stance towards cryptocurrencies and blockchain technology regulations, it has not issued its own cryptocurrency or backed any specific digital asset. The Government, however, engaged two providers to assist with the creation of a private government blockchain that would attempt to integrate blockchain technology into the eGov system in a bid to cut costs and red tape. The initial focus was to enable citizens to securely interact with government departments using their digital identity.

Cryptocurrency regulation

Gibraltar has experienced significant growth in the DLT industry and has solidified its status as a blockchain-friendly jurisdiction. The DLT Regs seek to regulate firms that store or transmit value (i.e. cryptocurrencies) belonging to others using blockchain technology (i.e. DLT) from Gibraltar. In its rawest form, the DLT Regs seek to capture entities that are providing exchange services and/or custodian services. Several blue chips have now set up operations in Gibraltar. These include Xapo, Tap Global, LMAX, Huobi, and eToro. While

token sales are not captured by the DLT Regs, they are now required to register with the GFSC and must undertake AML/CFT due diligence checks on all participants in line with POCA (more information below).

The GFSC regulates DLT Firms. The GFSC encourages DLT Firms wishing to operate in Gibraltar to adopt a proactive and transparent communicative relationship with the GFSC so that the GFSC can quickly get to grips with the underlying business during the application process. This assists with speed to market, something that the jurisdiction prides itself on.

The DLT Regs and the regulatory regime created by them is principles-based, with 10 core principles as follows:

1. A DLT Firm must conduct its business with honesty and integrity.
2. A DLT Firm must pay due regard to the interests and needs of each and all its customers and must communicate with its customers in a way that is fair, clear and not misleading.
3. A DLT Firm must maintain adequate financial and non-financial resources.
   While there are no specific requirements, the GFSC will want to be satisfied that DLT Firms have in place both financial and non-financial resources. As each case is different, a DLT Firm's resources are evaluated on a case-by-case basis having regard to the forecasts and risk.
4. A DLT Firm must manage and control its business effectively, and conduct its business with due skill, care and diligence, including having proper regard to risks to its business and customers.
5. A DLT Firm must have effective arrangements in place for the protection of client assets and money when it is responsible for them.
6. A DLT Firm must have effective corporate governance arrangements.
7. A DLT Firm must ensure that all systems and security access protocols are maintained to appropriate high standards.
8. A DLT Firm must have systems in place to prevent, detect and disclose financial crime risks, such as money laundering and terrorist financing.
9. A DLT Firm must be resilient and must develop contingency plans for the orderly and solvent wind-down of its business.
10. A DLT Firm must conduct itself in a manner that maintains or enhances the integrity of any markets in which it participates.

The GFSC states that the primary purpose of the DLT Regs is to create a safe environment for DLT Firms to operate and innovate, while simultaneously protecting consumers and safeguarding Gibraltar's reputation as a trusted and stable global business hub. The principles-based approach was designed to provide a robust framework with an optimum level of flexibility that is required in such a fast-moving industry. Five years on since its enactment, the jurisdiction has evolved and the licensing process has become more streamlined.

When a prospective DLT Firm is considering making an application to the GFSC, it is encouraged to arrange a pre-application meeting with the GFSC. The prospect will have an opportunity to discuss its business model and the exact nature of services to be offered. Once satisfied, the prospect is required to submit an initial application to the GFSC. The prospect shall submit an initial application form and business plan, which shall provide the GFSC with details of its prospective name, the type of business, products and services it intends to offer, the proposed operating address and the name and email of the main contact person for the application, along with a non-refundable initial application assessment fee. Details of the founders and key individuals should also be identified at this stage.

The GFSC will at this point determine the category that the firm falls into. This process usually takes approximately two weeks. There are a number of aspects considered when

categorising the prospect, which include the risks associated with the proposed business model. Once categorised, this will then dictate the respective application and annual fees payable to the GFSC.

Following this determination, the prospect is then able to pay the full application fee and submit an application pack to the GFSC along with all the relevant policy manuals and procedures, including application forms for each and every individual fulfilling a regulated function (this includes Directors, Shareholders and key management personnel).

Despite being at the forefront of the DLT revolution, Gibraltar's traditional fintech businesses are still growing, and Brexit has given Gibraltar the chance to offer a unique gateway on the European continent to offer services into the United Kingdom ("UK"). The common market that continues to exist between Gibraltar and the UK exists because of the historic and special relationship between Gibraltar and the UK. Gibraltar remains the only jurisdiction in a post-Brexit world to have direct access into the UK. Up until Brexit, all EU financial services legislation had been transposed into Gibraltar law and continues to apply irrespective of Brexit. Given Gibraltar's already highly regarded DLT Regs, it remains to be seen whether or not the Markets in Crypto-Assets Regulation (or "MiCA" as was adopted by the EU Council in October 2022) will be adopted (either in its entirety, partly, or not at all).

Sales regulation

Gibraltar has also sought to restrict Gibraltar firms or persons from selling digital assets, whether that be initial token offerings or over-the-counter ("OTC") offerings. Through subsidiary legislation of POCA, a person is now required to register with the GFSC before selling digital assets by virtue of the fact that they are considered to be undertaking a relevant financial business ("RFB").

The definition of an RFB includes:

- "[U]ndertakings that receive, whether on their own account or on behalf of another person, proceeds in any form from the sale of tokenised digital assets involving the use of distributed ledger technology or a similar means of recording a digital representation of an asset"; and
- "persons that, by way of business, exchange, or arrange or make arrangements with a view to the exchange of– (a) virtual assets for money; (b) money for virtual assets; or (c) one virtual asset for another."

In order to register, it is necessary to go through an application process with the GFSC, which requires the firm to submit an AML/CFT policy and manuals and application forms for each and every individual fulfilling a regulated function (Directors, Shareholders and Money Laundering Reporting Officers ("MLROs") (who must be Gibraltar based)).

Gibraltar law does not distinguish or categorise cryptocurrencies, but rather utilises the very broad terms of "virtual asset". Virtual asset means a digital representation of value that can be digitally traded or transferred and can be used for payment or investment purposes, but does not include digital representations of fiat currencies or financial instruments specified in paragraph 46 of Schedule 2 to the Financial Services Act 2019 ("FSA"). Should a token be considered a financial instrument, then one would need to consider the provisions of the FSA.

Taxation

Gibraltar does not levy capital gains tax, value-added tax, or withholding tax. Furthermore, there are certain personal tax statuses that can apply to individuals whereby one's individual income tax position is capped.

Gibraltar operates a territorial corporation tax model. Consequently, companies shall pay 12.5% corporation tax on all profits that are accrued in or derived from Gibraltar. In other words, if the profits do not accrue in or derive from Gibraltar, then they shall not be taxable in Gibraltar. A licensed entity is, by virtue of its licence, deemed to be operating in Gibraltar and consequently, all income that it accrues is deemed to accrue in and derive from Gibraltar.

It should be noted that neither Gibraltar's generally accepted accounting standards nor its current tax laws specifically address how cryptocurrencies should be treated. As a result, general principles implied by Gibraltar's existing laws and accounting standards that are deemed appropriate are applied.

Money transmission laws and anti-money laundering requirements

The Anti-Money Laundering Directives have been transposed into Gibraltar legislation and apply to all RFBs, which, for the avoidance of doubt, include DLT Firms and token-selling companies. RFBs are required to carry out customer due diligence ("CDD") and ongoing monitoring and risk assessments of their clients. Each RFB must appoint an MLRO to oversee and ultimately be responsible for the firm's checks and balances in this respect.

DLT Firms are required to establish and maintain appropriate and risk-sensitive policies, controls and procedures relating to: CDD measures and ongoing monitoring; reporting; recordkeeping; internal control; risk assessment and management; compliance management, including the allocation of overall responsibility for the establishment and maintenance of effective systems of control to a compliance officer at management level; and employee screening.

POCA states that CDD measures shall include identifying the customer and all beneficial owners, and understanding the ownership and control structure, obtaining information on the purpose and intended nature of the business relationship or occasional transaction, and taking a risk-based approach to the verification of the identity of the customer, all beneficial owners and the source of funds and wealth of the same.

In the case of a corporate or legal entity, CDD measures shall include obtaining its name, legal form and proof of existence, the powers that regulate and bind the corporate or legal entity, the names of the relevant persons in a senior management position, the address of its registered office and, if different, its principal place of business.

The "travel rule" applies to transfers of virtual assets (i.e. crypto assets) where the transaction has a value equal to or in excess of €1,000 and requires virtual asset service providers ("VASPs"), including cryptocurrency exchanges, digital wallet providers, OTC trading desks, and other companies dealing with crypto assets, to make sure that specific customer information is obtained, disclosed, and transferred between counterparties in a crypto asset transaction (more on this below).

Businesses in the fintech industry are now obligated to take the necessary steps to account for these regulations. For the purposes of AML/CFT, POCA also mandates that all pertinent financial businesses register with the GFSC. Registration of the MLRO and payment of a fee are part of this process.

Promotion and testing

There is no "sandbox" in Gibraltar. Instead, the GFSC may require DLT Firms to undertake a testing phase and a restricted operation phase in a controlled environment with regulatory oversight to prove the DLT Firm's concept. By doing so, DLT Firms can gain valuable insights, receive feedback from regulators, and potentially launch their services to the

market in a compliant manner. This fosters an environment of responsible innovation and helps Gibraltar to stay at the forefront of fintech and blockchain developments.

Additionally, Gibraltar's favourable regulatory environment for DLT Firms, as provided by the DLT Regs, also contributes to promoting research and investment in cryptocurrency and blockchain projects within the territory. Gibraltar acknowledges that this is a young industry, and while Gibraltar has demonstrated leadership in this area, development is undoubtedly a continuous process. Gibraltar is aware of the importance of investing in supporting knowledge and skill development, along with producing economic results, as it continues to strive for excellence in an effort to emulate that mindset in the blockchain realm.

Ownership and licensing requirements

A firm must be authorised by the GFSC under the DLT Regs if it is carrying out an activity for commercial gain that involves the storage or transmission of digital assets belonging to third parties.

Collective Investment Scheme ("CIS") legislation is another important legal factor to take into account if the objective is to create a structure that allows a number of investors to pool their assets and have them professionally managed by an independent manager rather than buying investments directly as individuals, and it must be noted that the participants of such an arrangement cannot have the day-to-day control over the management of the assets, with any property managed as a whole, and any profits or income must be pooled. A CIS is defined in the FSA as "any arrangement with respect to property, the purpose or effect of which is to enable persons taking part in the arrangement, whether by becoming owners of the property or any part of it or otherwise, to participate in or receive profits or income arising from the acquisition, holding, management or disposal of the property or sums paid out of such profits or income".

The most common fund structures in Gibraltar are Experienced Investor Funds ("EIFs") and Private Funds, and both vehicles can be used to invest in crypto assets. EIFs, in particular, are designed for high-net-worth and experienced investors. An EIF is required to appoint EIF Directors and licensed service providers. Furthermore, they can be structured as a Protected Cell Company ("PCC") or a Protected Cell Limited Partnership ("PCLP"). PCCs and PCLPs are vehicles that can establish numerous segregated cells and operate differing strategies, thereby segregating the assets and liabilities into separate cells. In addition, consideration must be made to the Financial Services (Alternative Investment Fund Managers) Regulations 2020. Gibraltar has enacted a dual regime that allows EIFs to safely opt out of the provisions of such Regulations.

Mining

There is no particular legislative or regulatory structure that specifically addresses the mining of Bitcoin and other cryptocurrencies; therefore, it is not generally a licensable activity. The manner in which the mining activity is carried out will need to be analysed to ensure that no licensing issues arise. Consideration will need to be given to the control that the miner has over the network/protocol and whether they are exercising control, therefore indirectly storing and transmitting valued by carrying out the act of mining.

Border restrictions and declaration

Other than the requirement that the DLT Firm must have its "mind and management" in Gibraltar, there are no specific border restrictions or obligations to declare cryptocurrency

holdings when entering or leaving the country. Gibraltar has been proactive in creating a regulatory framework for cryptocurrency businesses, aiming to attract companies in the blockchain and digital asset space.

Reporting requirements

The Government has implemented regulations to combat money laundering and terrorist financing, which include reporting obligations for certain transactions involving crypto-currencies.

DLT Firms are required to comply with AML/CFT obligations, which includes conducting CDD, monitoring transactions, and reporting suspicious activities.

In order to deal with the enactment of the "travel rule" outlined in the updated Recommendation 15 (read in conjunction with Recommendation 16) of the Financial Action Task Force ("FATF") Recommendations, Gibraltar has additionally introduced a number of pieces of legislation. RFBs as defined in s.9 POCA, which includes persons who send (on behalf of a "payer") or receive (on behalf of a "payee") virtual assets to or from VASPs, are now subject to the "travel rule" responsibilities. The RFB acting on behalf of the payer in a virtual asset transaction that has been covered by the regulations is required to collect and submit specific information regarding the payer and the payee, which the RFB will already have as part of its due diligence unless the payee is not one of its clients, with the RFB being obligated to obtain the payee's information from the originator RFB and confirm this with their internal records in respect of their name and, in some instances, their account number. However, when the RFB transmits a virtual asset transfer to someone other than a VASP, the travel rule does not apply. Other than the standard CDD measures that an RFB must satisfy under POCA, there are no information collection requirements in this circumstance. The regulations make it clear that any requirement under the regulations for an RFB to obtain the information, or any part of it, shall constitute a CDD measure, given the overlap between travel rule information and CDD information obtained during the normal course of an RFB's activities. Information gathered when sending or receiving virtual asset transfers is subject to the recordkeeping obligations under POCA as well.

Depending on whether an RFB is operating on behalf of a payer, a payee, or both (as well as on its own behalf), the information gathering needs to change slightly. When RFBs receive virtual asset transfers from someone other than a VASP (such as virtual assets acquired through an unhosted wallet), they must additionally take into account their obligations as well.

Estate planning and testamentary succession

For the purposes of estate planning and testamentary succession regarding cryptocurrency, there is no guidance as of yet. Gibraltar's succession law derives from the UK Wills Act 1837 and was enacted as the Wills Act, with the administration of estates enacted as the Administration of Estates Act 1948 (which consolidated the original 1933 Act).

In Gibraltar, people may establish trusts or include cryptocurrency in their wills as part of their estate planning in order to ensure the orderly transfer of their digital assets after death. To make the transfer procedure easier, it is crucial to precisely identify and specify the cryptocurrencies possessed, along with their wallet addresses and any other access details, and ensure the value is maintained. In addition, Gibraltar does not impose any duties payable upon death.

Jay Gomez
Tel: +350 200 72020 / Email: jay.gomez@triay.com

Jay Gomez is a Partner and forms part of the Corporate & Commercial and Financial Services teams. He has developed a strong reputation as an expert in financial services and regularly advises prospective funds, investment managers, insurance companies, insurance intermediaries, banks, e-money institutions and payment service providers on licensing requirements and regulatory, operational, passporting and distribution matters.

He has been elected on numerous occasions by the legal community in Gibraltar to represent them on the executive body of the Gibraltar Funds and Investment Association (GFIA) and is the Deputy Chairman of GFIA.

Jay has played an integral role in numerous changes to Gibraltar law, including the National Private Placement Rules, the Small AIFM Rules in Gibraltar following the implementation of the AIFM Directive, the Experienced Investor Funds Regulations and Brexit legislation.

Jay was instrumental in establishing the firm's FinTech team as one of the most highly regarded teams in Gibraltar.

Javi Triay
Tel: +350 200 72020 / Email: javi.triay@triay.com

Javi Triay is a Partner and forms part of the Financial Services team and the Shipping & Admiralty team. He has advised on a wide variety of financial services matters, which include establishing regulated entities and advising them on their applications to the GFSC. Notably, Javi was actively involved in the establishment of the first Gibraltar crypto fund to list on a recognised ESMA stock exchange.

Javi has been instrumental in establishing the FinTech team as one of the most highly regarded teams in Gibraltar. Furthermore, since the enactment of the distributed ledger technology regulations, he has been advising numerous blockchain start-ups (to include DLT licences and ICOs) and traditional financial services firms using blockchain technology on their establishment and regulatory position in Gibraltar.

Johnluis Pitto
Tel: +350 200 72020 / Email: johnluis.pitto@triay.com

Johnluis Pitto forms part of the Financial Services team. He completed his Bachelor of Laws with Honours at Manchester Metropolitan University, graduating with a First-Class Honours in 2021 and a Master of Laws in Professional Legal Practice through the University of Law, graduating with a Distinction with his Master's element in 2022. Thereafter, he successfully completed the Professional Skills Course and the Professional Certificate of Competence in Gibraltar Law, also graduating with a Distinction.

Prior to joining the firm, Johnluis worked as a Legal Executive for a Corporate and Fund Service firm, gaining a wealth of experience in company and funds administration. He also was a private in the Royal Gibraltar Regiment's Territorial Army. Johnluis joined the firm in September 2022 and has completed seats in corporate & commercial, property, private client and dispute resolution, while also assisting the Financial Services team.

Triay Lawyers Limited

28 Irish Town, Gibraltar, GX11 1AA, Gibraltar
Tel: +350 200 72020 / URL: www.triay.com

Hong Kong

Gaven Cheong & Esther Lee, Tiang & Partners
Peter B. Brewin & Duncan G Fitzgerald, PwC Hong Kong

Government attitude and definition

Government attitude

Over the course of the last four years, Hong Kong's regulators have been expanding their jurisdiction and remit over activities in relation to cryptocurrencies with a view to not only offering better investor protection, but also building a harmonised regulatory framework across the entire ecosystem such that Hong Kong is becoming a hub for cryptocurrency activity in the region.

In 2018, the Securities and Futures Commission (the "**SFC**") (Hong Kong's securities regulator) introduced a compulsory licensing regime for the management of portfolios of virtual assets ("**VAs**") in circumstances where managers that were already licensed for traditional securities management propose to include VAs in their portfolio in excess of 10% or more of the gross value of their assets under management ("**AUM**").

At the same time, recognising that the limit of its jurisdictional reach only extended to assets that are defined as "securities" under the Securities and Futures Ordinance (Cap. 571) (the "**SFO**") (and that many VAs do not fall into this category but are, instead, more likely to be "utility tokens"), the SFC also introduced an "opt-in" regime for managers not previously licensed for traditional asset management, who now want to become VA managers and regulated by the SFC.

In 2019, the SFC further launched an opt-in licensing regime (the "**Opt-in Regime**") for virtual asset service providers ("**VASPs**") looking to operate VA exchanges in Hong Kong. In addition, most recently in June 2023, the SFC implemented a mandatory licensing regime for VA trading platform operators ("**VATPs**") that seek to (a) hold client assets, and (b) provide services (by electronic means) whereby (i) offers to sell or purchase VAs are regularly made or accepted, or (ii) persons are regularly introduced to each other for the purpose of negotiating or concluding sales or purchases of VAs (in each case in the manner that results in a binding transaction).

In line with the expanding net of regulations over cryptocurrency activity and services, there has been an increasing number of participants (managers, traders, exchanges, etc.) applying for and receiving licences from the SFC. As of 7 August 2023, the SFC has issued 11 Type 9 VA licences (for management of a portfolio of 100% VAs), and at least one hybrid licence for a Type 9 asset manager to manage a fund of crypto funds.

In January 2022, the SFC and the Hong Kong Monetary Authority (the "**HKMA**") (Hong Kong's central banking institution) issued a joint circular (the "**Joint Circular**") expanding the reach of regulation to various other types of regulated activity involving VAs, including

distribution activities, dealing services and advisory services, and requiring these service providers to comply with additional requirements, such as ensuring suitability, providing risk-related disclosures and conducting proper due diligence when providing services in relation to VAs.

In January 2023, the HKMA announced a mandatory licensing regime for entities carrying on regulated activity in relation to an "in-scope" stablecoin. Regulated activities include governance, issuance, stabilisation and provision of wallet services in relation to stablecoins. Such mandatory licensing regime is expected to come into force in 2024/25 before which, a more detailed consultation will be conducted (the "**Mandatory Stablecoin Licensing Regime**").

From all of the above, it is clear that government attitude in Hong Kong to cryptocurrency activity is welcoming and inclusive with appropriate regulation. Of particular note is the fundamental (and significant) shift to allow retail access to "non-security" VAs that are traded on licensed VATPs in the near future. Further, amid the turmoil surrounding the implosion of FTX, the SFC has followed through with its proposal to authorise VA futures exchange-traded funds ("**ETFs**") (CSOP Bitcoin Futures ETF (3066) and CSOP Ether Futures ETF (3068) in December 2022 and Samsung Bitcoin Futures Active ETF (3135) in January 2023) for public offering. Other than these instances, however, across all the other different types of regulatory licences that have been issued so far (and in respect of all the other different regimes), the provision of services is still restricted only to "professional investors".[1] Importantly, to date, there are no spot VA products that have been approved for retail consumption (even if they are listed on a licensed VATP). However, some VA-related derivative products have been authorised for offer to retail investors (please see "Distribution of VAs" below). We expect this trend to continue at least in the short to medium term.

Definition

Under Hong Kong law, cryptocurrencies are not legal tender regulated by the HKMA and do not qualify as money. There is currently no digital asset that is backed by the Hong Kong government. In the Joint Circular, the SFC and the HKMA adopted the definition in the SFC's Position Paper published on 6 November 2019, referring broadly to "VAs" as digital representations of value that may be in the form of:

(i) digital tokens (such as utility tokens, stablecoins or security- or asset-backed tokens); or
(ii) any other virtual commodities, crypto assets or other assets of essentially the same nature,

irrespective of whether or not they amount to "securities" or "futures contracts" as defined under the SFO. However, digital representations of fiat currencies issued by central banks were expressly excluded from the definition of "VAs".

In Hong Kong's Anti-Money Laundering and Counter-Terrorist Financing Ordinance (the "**AMLO**"), "VA" is defined in more detail as a digital representation of value that:

(a) is expressed as a unit of account or a store of economic value;
(b) (i) functions (or is intended to function) as a medium of exchange accepted by the public (1) as payment for goods or services, (2) for the discharge of a debt, or (3) for investment purposes, or (ii) provides rights, eligibility or access to vote on the management, administration or governance of any cryptographically secured digital representation of value; and
(c) can be transferred, stored or traded electronically (e.g. Bitcoin or other stablecoins).

Such definition is consistent with the one adopted by the Financial Action Task Force (the "**FATF**") and will include cryptocurrencies.

The AMLO has also explicitly carved out, from the definition of VA, a digital representation of value that (i) is issued by central banks, (ii) constitutes securities or a futures contract that are already regulated under the SFO, (iii) constitutes a stored value facility, or (iv) is a limited purpose digital token ("**LPDT**"). In the Financial Services and the Treasury Bureau's (the "**FSTB**") Consultation Conclusions, LPDTs are defined as assets that are non-transferable, non-exchangeable and non-fungible in nature. In line with the FSTB's interpretation, the AMLO further provides that LPDTs include (i) customer loyalty or reward points, (ii) in-game assets, and (iii) tokens similar to (i) and (ii) that are not intended to be convertible into money or another medium of exchange accepted by the public.

Importantly, in a circular[2] issued on 1 November 2018, the SFC drew the distinction between utility and security tokens (see further below).

Stablecoins

Stablecoins are generally considered a subset of VAs and are also currently not legal tender in Hong Kong.

In the Conclusion of Discussion Paper on Crypto-assets and Stablecoins published in January 2023, the HKMA proposed a Mandatory Stablecoin Licensing Regime requiring entities to obtain a licence from the HKMA if: (a) they conduct a regulated activity in Hong Kong; (b) they actively market a regulated activity to the Hong Kong public; (c) they conduct a regulated activity concerning a stablecoin that references the value of the Hong Kong dollar regardless of whether such regulated activity is conducted in Hong Kong or actively marketed to the Hong Kong general public; or (d) the HKMA considers that they should be regulated, having regard to "matters of significant public interest".

In terms of which stablecoins will be regarded as "in scope", the HKMA will prioritise the regulation of stablecoins that reference one or more fiat currencies, irrespective of the underlying stabilisation mechanism. However, flexibility will be built in to enable the HKMA to include other types of stablecoins in the Regime in the future. For instance, the HKMA may publish "guiding factors" that would be considered when determining whether a particular stablecoin structure is "in scope".

Cryptocurrency regulation

In Hong Kong, cryptocurrencies are considered a form of VA that are generally categorised either as security tokens or non-security tokens (e.g. utility tokens). Starting from 1 June 2023, non-security tokens are regulated in Hong Kong by the SFC to the extent that a party proposes to operate a VATP in Hong Kong (or offer VATP services into Hong Kong), even if that VATP will only list non-security tokens for trading. This is the first time the SFC has extended its jurisdiction over assets that are non-securities (as defined under the SFO).

Security tokens

Security tokens are also known as "tokenised securities". Depending on the extent and type of activities, activities in relation to these security tokens may be considered "regulated activities" that can only be carried out with the relevant licence(s) issued by the SFC (e.g. dealing in and advising on security tokens).

Cryptocurrencies will be deemed security tokens if they fall within the definition of "securities" under the SFO. In its Statement on initial coin offerings (5 September 2017),[3] the SFC further clarified that digital tokens (including any cryptocurrencies) may be considered "securities" if they:

- represent equity or ownership interests in a corporation;
- create or acknowledge a debt or liability owed by the issuer;

- pay regular returns to investors that amount to dividend or interest; or
- give their holders rights akin to that of a creditor or a shareholder (e.g. voting rights or the right to participate in the distribution of the corporation's surplus assets upon winding up).

Therefore, most stablecoins and cryptocurrencies (e.g. Bitcoin and Ether) in the market are not regarded as securities according to the definition under the SFO.

Non-security tokens

In contrast, cryptocurrencies other than security tokens are considered "non-security tokens" or "virtual commodities".

Mandatory VASP Licensing Regime

On 7 December 2022, the Legislative Council passed the Anti-Money Laundering and Counter-Terrorist Financing (Amendment) Bill 2022 (the "**Amendment Bill**"), which implemented a mandatory licensing regime for VASPs (the "**Mandatory VASP Licensing Regime**") expanding its jurisdiction to cover the trading of non-security tokens. Under the Mandatory VASP Licensing Regime, a person operating a VA exchange in (a) Hong Kong, or (b) elsewhere but actively markets to the Hong Kong public, will be regarded as carrying out a "regulated activity" (regardless of whether the VAs in question are "security" or "non-security" tokens) for which a licence from the SFC is required.

On 1 June 2023, the SFC published the Guidelines for VATPs that set out details of the Mandatory VASP Licensing Regime, including rules allowing licensed VATPs to allow access by retail customers to the trading of non-security VAs. Below lists the prerequisites to be additionally fulfilled for retail access to VAs by VATPs:

- prior to token admission:
  - (a) admission of VAs for trading by retail investors only if the following criteria are met:
    - (i) the VA does not fall within the definition of "securities" under the SFO;
    - (ii) the VA is of high liquidity, making it an eligible large-cap VA (included in a minimum of two acceptable indices issued by at least two different index providers); and
    - (iii) written approval is obtained from the SFC;
- prior to opening of accounts:
  - (b) assessment of the retail investors' knowledge in VAs and their associated risks, and should this knowledge be lacking, provision of adequate training to the retail investor;
  - (c) satisfaction of know-your-client procedures, including establishment of the true and full identity, financial situation, investment experience and investment objectives of the retail investor, assessment of the investor's risk tolerance level and risk profile relevant to the services to be provided; and
  - (d) establishment of a limit with reference to the retail investor's financial situation and personal circumstance;
- prior to provision of services:
  - (e) entering into of a written client agreement containing certain specified terms; and
- when making recommendation or solicitation:
  - (f) ascertainment of the suitability of such recommendation or solicitation, having regard to information of which the VATP is or should be aware; and
  - (g) disclosure obligations – all reasonable steps should be taken to disclose, in a prominent manner, the nature and risks exposed in trading VAs and using the services provided by the VATP.

In line with the existing licensing regime for carrying out regulated activity under the SFO, the Mandatory VASP Licensing Regime also imposes certain baseline requirements on potential applicants. For instance, applicants must: (1) have sufficient presence in Hong Kong; (2) appoint at least two responsible officers ("**ROs**") to ensure compliance with the anti-money laundering ("**AML**") and counter-terrorist financing ("**CTF**") requirements under the AMLO, and appoint at least one of the ROs as an executive director of the applicant; and (3) meet the fit-and-proper test.

On granting a VATP licence, the SFC may impose any conditions on the licence, including but not limited to (a) financial resources, (b) knowledge and experience, (c) risk management policies and procedures, (d) AML/CTF policies and procedures, (e) management of client assets, (f) soundness of business, (g) financial reporting and disclosure, (h) VA listing and trading policies, (i) prevention of market manipulation and abusive activities, (j) avoidance of conflicts of interests, (k) keeping of records and accounts, and (l) cybersecurity. Some key features of the regime include:

- limitation of scope of non-security tokens to retail investors;
- prohibition of providing algorithmic trading services;
- prohibition of making arrangements to use the investors' VAs to generate returns for the clients or any other parties (e.g. staking, lending and borrowing);
- prohibition of offering, trading or dealing activities in VA futures contracts or related derivatives; and
- no admission of stablecoins for retail trading until regulatory arrangements in respect of stablecoins are in place.

The Mandatory VASP Licensing Regime took effect on 1 June 2023 (the "**Effective Date**") with transitional arrangements available to certain qualified unlicensed exchanges that had established a significant presence and operations in Hong Kong prior to the Effective Date.

VA management

In October 2019, the SFC introduced a new licensing regime for businesses directly managing a portfolio of VAs (the "**Type 9 VA Licensing Regime**").

Under the Type 9 VA Licensing Regime, managers who currently hold a regular Type 9 (Asset Management) licence ("**Type 9 Licence**") ("**Type 9 Managers**"), and who seek to directly manage a portfolio of VAs that account for 10% or more of the portfolio's gross asset value ("**GAV**"), must expand their licences to a Type 9 VA licence with additional terms and conditions[4] (the "***Pro Forma* T&Cs**") imposed on their existing Type 9 Licences. The *Pro Forma* T&Cs provide for, among other things, general principles relating to VA fund management, organisation and management structure of VA fund managers, management rules (e.g. best execution, prohibition on market misconduct, order allocation, participation in initial offerings, cross trades, risk management, leverage, liquidity management), custody of portfolio assets and client monies, record keeping, audits, portfolio valuation, marketing activities, fees and expenses, and reporting obligations to the SFC.

However, Type 9 Managers managing a portfolio of VAs that account for less than 10% of the portfolio's GAV will only need to notify the SFC that they intend to manage such VAs (without requiring the SFC's consent).

New managers who wish to manage a portfolio of pure VAs (regardless of whether their portfolios consist of any "securities") may also choose, but are not required, to apply for a Type 9 VA licence and subject themselves to the jurisdiction of the SFC.

Managers with a Type 9 VA licence ("**Type 9 VA Managers**") are subject to different restrictions imposed by the SFC. For instance, Type 9 VA Managers can only manage VA portfolios for "professional investors". There is also a minimum liquid capital requirement of HK$3 million and minimum paid-up capital requirement of HK$5 million for Type 9 VA Managers. Following the Effective Date of the Amendment Bill, Type 9 VA Managers are expected to choose licensed VASPs if they wish to trade VAs through trading platforms.

In addition, Type 1 (Dealing in Securities) licensed corporations ("**Type 1 Intermediaries**") who manage funds solely investing in VAs that are not "securities" or "futures contracts" and distribute the same in Hong Kong must also adhere to the *Pro Forma* T&Cs[5] on their licences.

Crypto fund of funds

For new managers who wish to manage a crypto fund of funds, the SFC has a "halfway house" regime, which does not require the incorporation of *Pro Forma* T&Cs but imposes requirements in addition to that of a regular Type 9 Licence, such as restricting the provision of services to "professional investors" only and prohibiting managers from holding "client assets" as defined under the SFO.

Sales regulation

Please refer to "Definition" and "Cryptocurrency regulation" above for the current and future regulatory framework on trading cryptocurrencies on exchanges and the licensing regime for management of funds in relation to VAs.

Distribution of VAs

In the Joint Circular, the SFC and the HKMA confirmed that VA products are likely to be considered "complex products" under the SFO. As such, distribution of any VA products must comply with the SFC's guidelines, such as (a) ensuring suitability, (b) providing specific risk-related disclosures, and (c) conducting proper due diligence on the product (including their risks and features, the investor target and the regulatory status). When distributing VA products, intermediaries must ensure their clients have sufficient net worth to be able to assume the risks and bear the potential losses of trading VA products (the "**Sufficient Net Worth Requirement**"), and where VA products are offered on online platforms, there are appropriate access rights and controls to ensure compliance with selling restrictions.

For VA derivatives, intermediaries must comply with the additional requirements under paragraphs 5.1A and 5.3 of the Code of Conduct for Persons Licensed by or Registered with the SFC (such as the Sufficient Net Worth Requirement and the client's knowledge requirement, both in relation to "derivatives" specifically).

Overseas VA non-derivative ETFs or other ETFs that invest directly in VAs are also considered complex products in the Joint Circular and must only be offered to "professional investors" subject to suitability requirements. However, a limited number of overseas VA-related derivative products that are traded on SFC-specified exchanges and have been approved for retail distribution by their relevant home regulators may be distributed to retail investors without the need for complying with the suitability requirements.

Nevertheless, when intermediaries distribute VA products that are complex products to individual "professional investors", they must (a) ensure that the clients have sufficient knowledge about VA investments (the "**VA Knowledge Test**"), and if the client does not, (b) proceed only (i) when it is in the client's best interests, and (ii) when the intermediary has provided relevant training to the client.

Finally, where an intermediary is providing financial accommodation in relation to VA products, it must ensure that the client has the financial capacity to meet obligations arising from leveraged or margin trading in such VA products.

Dealing in VAs

Dealing services in relation to VAs that are "securities" can only be provided by Type 1 Intermediaries. However, the SFC has stated that the services of dealing in non-security VAs fall outside the SFC's jurisdiction, implying that such services may be provided by non-intermediaries.

When providing VA dealing services, Type 1 Intermediaries must only partner with SFC-licensed VATPs and must not allow clients to withdraw or deposit fiat currencies from their accounts held by the intermediaries. Type 1 Intermediaries must also only provide VA dealing services to "professional investors" who are existing clients to whom the Type 1 Intermediary is providing Type 1 dealing services. When they act as introducing agents to SFC-licensed platforms, Type 1 Intermediaries should only introduce "professional investors" and cannot relay order or hold client assets.

In addition, Type 1 Intermediaries must comply with Part I of the terms and conditions set out in Appendix 6 to the Joint Circular,[6] which impose some general requirements (such as record keeping, audit, AML/CTF and ongoing reporting obligations) and some specific requirements in relation to VAs, which require intermediaries to:

(i) maintain excess liquid capital equal to 12 months of their actual operating expenses calculated on a rolling basis;
(ii) establish omnibus accounts for clients designated as trust or client accounts on SFC-licensed VA platforms;
(iii) have client agreement with specific disclaimers and disclosures in place;
(iv) hold VAs on trust in segregated accounts on SFC-licensed platforms; and
(v) hold client money in segregated bank accounts.

Taxation

Hong Kong adopts a territorial principle of taxation, where only a person carrying on a business in Hong Kong and deriving profits sourced in Hong Kong from that business are liable to Hong Kong profits tax (at a tax rate of 15% for unincorporated businesses and 16.5% for corporations). It is characterised by key features such as no turnover tax (e.g. value-added tax, goods and services tax), no capital gains tax, generally no tax on dividend income, and no withholding tax on dividends and interest. From 1 January 2023, four types of offshore passive income, namely dividends, interest, disposal gains in relation to shares or equity interest, and income from intellectual property ("**IP**"), received in Hong Kong will continue to be non-taxable only if certain conditions (e.g. economic substance requirement for non-IP income, nexus approach for IP income) are met.

Taxation of cryptocurrencies

While no specific laws are in place on the taxation of cryptocurrencies, the Inland Revenue Department (the "**IRD**") issued the revised Departmental Interpretation and Practice Notes No. 39 ("**DIPN 39**") in March 2020, which provides guidance on the digital economy, electronic commerce and digital assets. The following are highlights of the section on the taxation of digital assets:

- The profits tax treatment of digital assets depends on their categorisation (payment token, security token or utility token).

- The proceeds of an initial coin offering are taxed by following the attributes of the token that is issued. If security tokens are issued, proceeds would generally be considered capital in nature. If utility tokens are issued, proceeds would generally be taxable if found to be sourced in Hong Kong.
- Digital assets held for long-term investment purposes may be considered capital in nature, in which case their disposal would result in capital gains (which are not taxable in Hong Kong). Whether digital assets are held for long-term investment purposes or as trading stock depends on the facts and circumstances with reference to well-established principles such as the "badges of trade", and the intention at the time of acquisition is always relevant.
- New cryptocurrencies received in the course of a cryptocurrency business (e.g. airdrops and blockchain forks) are to be regarded as receipts of the business and assessed accordingly.
- Cryptocurrency received by an employee as employment income should be reported at its market value and subject to the same salaries tax treatment as regular remuneration.

As the revised DIPN 39 was issued in 2020, it does not cover issues arising from more recent developments such as decentralised finance ("**DeFi**"), staking and non-fungible tokens ("**NFTs**"). As it generally takes longer for the IRD to update a DIPN, future guidelines may potentially be provided in the form of frequently asked questions ("**FAQs**") on the IRD's website.

VA funds and the Unified Fund Exemption

The list of qualifying assets included in the Unified Fund Exemption regime includes securities and other types of financial products. As most digital assets are not considered securities, these would not be qualifying assets for purposes of the exemption.

VA borrowing and lending

DIPN 39 does not address VA borrowing and lending. As cryptocurrency is generally not "stock", relief for stock borrowing and lending is not applicable. Also, as cryptocurrency is not "money", provisions in relation to "interest" that make reference to money are not applicable.

Money transmission laws and anti-money laundering requirements

Money transmission laws

There is currently no specific legislation in Hong Kong on the transfer of cryptocurrencies between private parties. However, if the transmission of cryptocurrencies includes the conversion into fiat currencies in substance, such transmission may be deemed a money remittance transaction, which will be subject to the AMLO. According to Section 3(1) Schedule 2 of the AMLO, a financial institution must carry out customer due diligence ("**CDD**") measures in relation to a customer for a wire transfer equal to or exceeding an aggregate value of HK$8,000, whether carried out in a single operation or several operations that appear to the financial institution to be linked. Records relating to CDD and transactions should be kept for at least five years from the date of transaction.

Anti-money laundering requirements

The AMLO in Hong Kong applies to financial institutions (including HKMA-authorised institutions (i.e. banks), SFC-licensed corporations, licensed insurance companies, stored value facility issuers and money service operators) and designated non-financial businesses and professions (for example, lawyers, certified public accountants, licensed estate agents,

and trust and company services agents). Thus, all SFC-licensed entities conducting regulated activities are subject to the AML/CTF obligations of the AMLO, which also include licensed VASPs under the new regime as mentioned above. The regulated bodies should also ensure compliance with the FATF's latest recommendation.

On the other hand, fund managers that manage funds investing only in cryptocurrencies that are not securities or futures contracts will not require a Type 9 Licence because this will not be considered a regulated activity. Since they are not licensed entities, they will not be subject to AMLO requirements. This is also reinforced by the Statement[7] in relation to "Bitcoin" and Money Service Operator Licence issued by the Money Service Supervision Bureau of the Customs and Excise Department (the "**CED**") in April 2014, in which the CED stated that, for the purposes of the AMLO, Bitcoin or other similar virtual commodities are not "money" and fall outside its jurisdiction.

Promotion and testing

On 29 September 2017, the SFC issued a circular[8] to announce the establishment of the SFC Regulatory Sandbox (the "**Sandbox**"). The aim of the Sandbox was to provide licensed corporations and startup firms with a confined regulatory environment in which to operate regulated activities under the SFO before any financial technology ("**Fintech**") is used on a fuller scale.

Initially, the SFC invited interested VASPs that had already obtained a Type 1 (Dealing in Securities) licence together with a Type 7 (Automatic Trading Services) licence to participate in the Sandbox. The SFC then closely monitored the performance of the qualified platform operator for a minimum of 12 months, after which they could apply to leave the Sandbox so as to be regulated in the same way as other licensed providers of automated trading services operating outside of the Sandbox. During the 12-month period, the VASP also had to list at least one VA token that had features of a "security" as defined under the SFO (that is, a "security token"). OSL Digital Securities Limited became the first participant to successfully take part in this sandbox regime and became the first SFC-licensed VA exchange in Hong Kong.

Similarly, the HKMA launched the Fintech Supervisory Sandbox on 6 September 2016 to facilitate the pilot trials of Fintech and other technology initiatives of authorised institutions before they are launched on a fuller scale.

Ownership and licensing requirements

Currently, there is no restriction on businesses or individuals simply owning cryptocurrencies, for investment or otherwise. Of note is that cryptocurrency ownership is subject to the laws and regulations in relation to digital assets in force in Hong Kong as set out above – and this is especially so where VAs also amount to "securities" as defined under the SFO (please see above).

Mining

There is currently no regulation on the mining of cryptocurrencies in Hong Kong. However, due to the scarcity of land in Hong Kong, there are certain restrictions on land use when leasing industrial buildings for the set-up of data centres or cryptocurrency mining centres (depending on the scale of the operation). Miners may be required to apply for a lease modification or a temporary waiver if such proposed use is not yet permitted. Moreover,

since mining activity is typically conducted by computers running continuously and will require an intensive electric power supply, miners should ensure that the building in which they are operating is in compliance with the Buildings Energy Efficiency Ordinance (Cap. 610). Considering the relatively high operating cost in Hong Kong, it will be more cost effective for crypto-mining operations to be held in environmentally friendly mining sites in North America and Asia.

Border restrictions and declaration

There is no obligation to declare cryptocurrency holdings when passing through Hong Kong Customs. According to the Cross-boundary Movement of Physical Currency and Bearer Negotiable Instruments Ordinance (Cap. 629), for any person arriving in Hong Kong at a specified control point and in possession of a large quantity of currency and bearer negotiable instruments ("**CBNIs**") of a total value of more than HK$120,000, a written declaration must be made to a Customs officer. However, since cryptocurrency is not considered a note or coin that is legal tender in Hong Kong, nor is it a negotiable instrument that is (1) in bearer form, (2) endorsed without any restriction, (3) made out to a fictitious payee, (4) in a form under which the title of it passes on delivery, or (5) signed but does not state a payee's name under the definition of "CBNI", it would appear unlikely to be mandatory to declare cross-border cryptocurrency holdings.

Reporting requirements

There is no reporting requirement for cryptocurrency payments in Hong Kong.

The CDD measures as required under the AMLO will only be triggered if there is an exchange of fiat currency of an amount equal to or above HK$8,000. As mentioned in "Money transmission laws" above, financial institutions should retain records relating to CDD and transactions for at least five years from the date of transaction and report any suspicious transactions.

Estate planning and testamentary succession

Under Hong Kong law, all of a deceased's property will pass to the beneficiaries according to a valid will made pursuant to the Wills Ordinance (Cap. 30) or, in the absence of a will, be distributed in accordance with the Intestates' Estates Ordinance (Cap. 73). Inheritance tax was abolished in 2006.

In general, property can be categorised as (i) movable, (ii) immovable, (iii) tangible, or (iv) intangible property. The rules of determining the governing law of succession will differ depending on the category in which the relevant property falls.

The Hong Kong courts have recognised cryptocurrency as a form of property since proprietary remedies were granted in a fraud case involving cryptocurrency.[9] As such, the treatment of cryptocurrency upon an owner's death is likely to follow the general succession rule in Hong Kong applicable to all other property as discussed above.

In line with the other common law jurisdictions, cryptocurrency, as a type of VA, is likely to be treated as intangible property due to its nature of being "an identifiable thing of value",[10] such that the law of the jurisdiction in which the cryptocurrency is located would not apply (in contrast with immovable property).

Nevertheless, thorough estate planning should be carried out to ensure that the value of cryptocurrency can be transferred upon the user's death (since funds in the crypto wallet may be irrevocably lost when hard drives are misplaced or private keys not safely kept).

Endnotes

1. According to Part 1 of Schedule 1 to the SFO and the Securities and Futures (Professional Investor) Rules, "professional investors" include classes of persons that can be broadly categorised into (1) institutional professional investors (including SFC-licensed or SFC-registered institutions, funds, financial institutions, insurance companies and recognised exchange companies), (2) corporate professional investors (including (i) corporations and partnerships with a portfolio of at least HK$8 million or total assets of at least HK$40 million, (ii) investment holding subsidiaries of "professional investors", and (iii) trust corporations), and (3) individual professional investors who have a portfolio of at least HK$8 million.
2. SFO/IS/061/2018.
3. https://www.sfc.hk/en/News-and-announcements/Policy-statements-and-announcements/Statement-on-initial-coin-offerings
4. *Pro Forma* terms and conditions for licensed corporations that manage portfolios that invest in VAs, published by the SFC in October 2019.
5. Please refer to the "Cryptocurrency regulation – VA management" section above for a summary of the *Pro Forma* T&Cs.
6. "Licensing or registration conditions and terms and conditions for licensed corporations or registered institutions providing virtual asset dealing services and virtual asset advisory services" published by the SFC in January 2022.
7. https://www.msoa.hk/docs/circulars/20140426/Statement%20on%20Bitcoin%20&%20MSO%20Licence%20(English).pdf
8. https://apps.sfc.hk/edistributionWeb/gateway/EN/circular/doc?refNo=17EC63
9. *Nico Constantijn Antonius Samara v Stive Jean Paul Dan* [2022] HKCFI 1254.
10. *B2C2 Ltd v Quoine Ptd Ltd* [2019] SGHC (I) 03.

* * *

Acknowledgments

Special thanks to the following for their contribution to this chapter: Karen Austin and Natalie Ng from Tiang & Partners; and Gwenda Ho, Ollie Roberts and Tommy Hui from PwC Hong Kong.

Gaven Cheong
Tel: +852 2833 4993 / Email: gaven.cheong@tiangandpartners.com
Gaven is Head of Investment Funds at Tiang & Partners, an independent Hong Kong law firm and a member of the PwC network.
In addition to working on a large number of traditional hedge and PE fund launches, Gaven is a pioneer in the crypto fund formation and regulatory advice space, having acted for the VSFG group (Arrano Capital) in getting Hong Kong's first Type 9 VA licence, and before that, Diginex in obtaining Hong Kong's first Type 9 (Asset Management) licence for managing a fund of crypto funds. In addition to his regulatory work, Gaven has also acted as lead international counsel for a large number of managers in setting up crypto funds, including clients such as the Spartan group, Moonvault, Anduril and IDEG.

Esther Lee
Tel: +852 2833 4950 / Email: esther.yt.lee@tiangandpartners.com
Esther is a Registered Foreign Lawyer (Counsel equivalent) at Tiang & Partners, an independent Hong Kong law firm and a member of the PwC network.
With more than 13 years of experience in investment funds, Esther advises on the establishment and operations of various fund structures, from private funds (PE and hedge) through to retail funds (authorised funds and ETFs), and the related regulations.
Esther is admitted in England & Wales and Queensland, Australia. She is fluent in English, Cantonese and Mandarin.

Peter B. Brewin
Tel: +852 2289 3650 / Email: p.brewin@hk.pwc.com
Peter is a Partner at PwC Hong Kong and has been working as part of PwC's core crypto advisory team since 2017. He is a keen believer that recent developments in NFTs, blockchain technology and AR/VR will remake the internet and open up game-changing value for participants. He has significant experience of advising companies in the blockchain and digital assets sector and has a particular interest in the regulatory and taxation challenges that arise from this new technology.

Duncan G Fitzgerald
Tel: +852 2289 1190 / Email: duncan.fitzgerald@hk.pwc.com
Duncan is an experienced practitioner and advisor in the areas of corporate governance, internal audit, internal control consulting and regulatory compliance. He has worked at PwC Hong Kong since 1996 and has been a Partner since 1999. He advises numerous organisations on corporate governance and internal controls using digital assets, also referred to as "crypto" (either as investors, issuers or exchanges) and has worked in this area since 2017/18. Duncan co-led the PwC Hong Kong team assisting the HKMA with its mCBDC project and has also worked with an extremely large crypto client on various aspects of their business.

Tiang & Partners
(an independent law firm and a member of the PwC network)

Room 2010, 20/F Edinburgh Tower, The Landmark,
15 Queen's Road Central, Hong Kong
Tel: +852 2833 4900 / URL: www.tiangandpartners.com

PwC Hong Kong

21/F Edinburgh Tower, The Landmark,
15 Queen's Road Central, Hong Kong
Tel: +852 2289 8888 / URL: www.pwchk.com

India

Nishchal Anand, Pranay Agrawala & Dhrupad Das
Panda Law

Government attitude and definition

Introduction

India has not enacted any special legislation for the regulation of virtual currencies ("**VCs**"). However, it has contemporised various statutes like the Companies Act, 2013, necessitating the reporting of virtual digital assets ("**VDAs**") in an effort to reflect the emerging dynamics of the financial landscape. It has also broadened the scope of the Prevention of Money Laundering Act, 2002 ("**PMLA**") by incorporating transactions related to VDAs, including various exchanges, transfers, and administrative measures associated with VDAs, as well as covering participation in, and the provision of, financial services linked to an issuer's offering and sale of a VDA. Alongside this, India's income tax laws have undergone significant modifications to include the taxation of VDAs, thereby recognising the fiscal implications of the burgeoning VC market.

In India, VDAs have gained substantial recognition on the legal front, further legitimising the industry. Enforcement actions under existing tax laws have been initiated, and anti-money laundering ("**AML**") laws have been expanded to encompass the burgeoning Web3/VDA industry. The concerted effort of financial and regulatory authorities worldwide mirrors the evolving significance and acceptance of the VDA industry.

In contrast, the stance of the government towards VDAs, which was to become clearer once the proposed bill titled *The Cryptocurrency and Regulation of Official Digital Currency Bill, 2021* became available to the public, is still awaited. Public statements made by high-ranking government officials indicate the replacement of a domestic-facing law regulating VDAs in favour of a globally aligned, internationally synchronised one. India, as the G20 president, is leading the global crypto regulation discussions with the International Monetary Fund and other stakeholders, while addressing different views from emerging and developed economies. In this regard, the Indian government has released a note entitled the *Presidency Note as an input for a Roadmap on Establishing a Global Framework for Crypto Assets* for consideration of the G20 members.

To understand the current attitude of the Indian government, we must look at all the contemporaneous actions taken by it through its various ministries, departments, and representatives.

The National Strategy on Blockchain

In December 2021, an updated version of the *National Strategy on Blockchain* was released.[1] This strategy advocates the development of a national blockchain infrastructure, geographically distributed throughout the country, in an attempt to create infrastructure for providing "*blockchain as a service*".

RBI on macro-financial risks

On 28th June 2023, the Reserve Bank of India ("**RBI**"), in a chapter of its report titled *Chapter III: Regulatory Initiatives in the Financial Sector*,[2] addressed the risks associated with VDAs. These include: consumer protection; investor safety; market integrity; financial stability; and challenges specific to Emerging Markets and Developing Economies ("**EMDEs**"), such as monetary sovereignty and "*cryptoisation*". To tackle these risks, three main policy approaches have been proposed: (i) prohibition; (ii) containment; and (iii) regulation. RBI noted that a globally coordinated effort would be necessary to evaluate these risks, especially the macroeconomic challenges like loss of monetary control and local currency volatility that disproportionately affect EMDEs compared to advanced economies. As part of India's G20 presidency, a key objective seems to be to establish a global regulatory framework for unbacked cryptoassets, stablecoins, and Decentralised Finance ("**DeFi**").

CERT Guidelines

On 28th April 2022, the Indian Computer Emergency Response Team ("**CERT-In**"), operating under the Ministry of Electronics and Information Technology ("**MeitY**"), issued *Directions under sub-section (6) of section 70B of the Information Technology Act, 2000 relating to information security practices, procedure, prevention, response and reporting of cyber incidents for Safe & Trusted Internet*. These Directions were issued to augment and strengthen cybersecurity in India, requiring service providers, intermediaries, data centres, bodies corporate and government organisations to mandatorily report all cybersecurity incidents to CERT-In. The Directions directly impact the blockchain, VDA and Web3 industry, as all "*attacks or malicious/suspicious activities affecting systems/ servers/ networks/ software/ applications related to … Blockchain, virtual assets, virtual asset exchanges, custodian wallets …* " have to be mandatorily reported within six hours of knowledge of such incident. Further, all virtual asset service providers, virtual asset exchange providers and custodian wallet providers are required to mandatorily maintain all information obtained as part of Know-Your-Customer ("**KYC**") procedures and records of financial transactions for a period of five years.

Central Bank Digital Currency ("**CBDC**")

RBI has been a consistent proponent of creating India's CBDC called the e-Rupee, a vision now realised with the successful initiation of the Rupee CBDC pilot. This endeavour is bolstered by an enabling legal framework, achieved through amendments to the Reserve Bank of India Act, 1934. It has broadened the definition of "bank note" to encompass bank notes issued by RBI in both physical and digital forms, paving the way for RBI to issue its own CBDC.

Currently, 10 banks are participating in the wholesale CBDC pilot, and 13 banks are part of the retail pilot. Both of these initiatives have demonstrated promising results, allowing for the testing of various technical architectures, design choices, and use cases. As of 30th June 2023, the retail pilot had exceeded 1 million users and more than 262,000 merchants, underscoring the potential of this digital form of currency to spur innovation and efficiency.[3]

Prevention of money laundering

The purpose of the PMLA and the Prevention of Money-laundering (Maintenance of Records) Rules, 2005 ("**Rules**") is to prevent money laundering activities, provide for confiscation of property derived from money laundering, and bring the persons involved in money laundering to justice.

The Ministry of Finance, through a notification dated 7th March 2023 ("**PMLA Notification**"), brought every entity involved in the transaction of VDAs (including exchanges, custodians and wallet providers) under the purview of the PMLA and Rules. This gives authorities greater power to monitor and reconstruct encrypted transactions, including transfers outside of India. Such entities have also been brought under the purview of the reporting requirements under the PMLA and Rules, which are discussed in the reporting section below.

Notably, the PMLA only extends to the territory of India, hence it may be presumed that foreign cryptocurrency exchanges offering their services in India would not fall within the purview of the PMLA Notification.

Taxation

The most significant development for the blockchain, Web3 and VDA industry was the amendment of the Income Tax Act, 1961 ("**IT Act**"), which introduced an income taxation regime for "VDAs", a term defined by the said regulation.

Broadly, these amendments introduced: (a) the definition of the phrase "Virtual Digital Asset", which includes non-fungible tokens ("**NFTs**"), while excluding closed-system instruments like gift cards or vouchers, mileage points, reward points or loyalty cards, and subscriptions to websites, platforms or applications; (b) a 30% tax on income from the transfer of a VDA; (c) a withholding tax on the transfer of VDAs from one entity to another; (d) treatment of VDAs that are received as gifts; (e) guidelines for VDA Exchanges ("**Exchanges**") on how to effect the amendments to the IT Act; and (f) guidelines for peer-to-peer ("**P2P**") transactions.

For more details on the implications of the amendments to the IT Act, please see the "Taxation" section below.

Digital lending

RBI, through its Working Group on Digital Lending including Lending through Online Platforms and Mobile Apps, in recommendations titled *Recommendations of the Working group on Digital Lending – Implementation*,[4] raised concern regarding the operation of unregulated entities carrying out the activity of digital lending, and called for specific legislative and institutional interventions to be enacted by the government to curb lending activity being carried out by unregulated entities.

Parliamentary questions

The past few years have seen a slew of questions put by parliamentarians to the government, and the answers provided thereto lend an insight into the government's attitude towards cryptocurrencies, VDAs and the industry in general. A few takeaways from these recent responses given are:

a) the effective regulation or prohibition of inherently borderless cryptoassets in India, which currently lacks specific legislation, hinges on international cooperation to evaluate risks and benefits and establish common taxonomy and standards, thereby mitigating regulatory arbitrage;[5]
b) the government is not collecting data on investment in cryptocurrencies or on cryptocurrency exchanges;
c) the government has investigated 11 exchanges for evasion of the goods and services tax ("**GST**"), from which a sum of INR 95.86 crores (approx. USD 12 million) has been recovered, including interests and penalties;
d) the Enforcement Directorate ("**ED**") has been investigating cases of money laundering where cryptocurrencies have been involved and has attached INR 135 crores (approx. USD 17 million) as "proceeds of crime";

e) the Narcotics Control Bureau and Central Board of Indirect Taxes and Customs has unearthed payments amounting to INR 2.2 crores (approx. USD 276,000), related to drug trafficking, that were made using cryptocurrencies;
f) the government is cognisant of the emergence of new technologies pertaining to Web3, such as blockchain, virtual reality, the metaverse, etc.; and
g) the infrastructure costs in the mining of VDAs will be in the nature of capital expenditure and will not be treated as acquisition costs, and hence will not allowable as deduction.

Impending contemporaneous legislation

Presently, the government is in the process of taking steps towards overhauling the entire legal architecture regulating the internet, big data, cybersecurity, telecommunication and data protection, and is accordingly introducing a fresh set of frameworks, policies and statutes. The overhaul of these laws and regulations, when complete, is likely to foster a positive environment for digital-first businesses in India. Such foundational laws in the pipeline today are as follows:

a) **Draft National Data Governance Framework Policy**[6] – This draft policy was published by the MeitY in May 2022, replacing the previous India Data Accessibility and Use Policy. The draft policy is intended to set up a framework for modernising how the government collects and handles data. This will ultimately lead to the creation of repositories of anonymised, non-private data sets, which would be useful for India's AI and blockchain ecosystem.
b) **Draft National Cyber Security Strategy**[7] – This policy has been drafted by the National Security Council Secretariat with a view to comprehensively addressing all current and future national cybersecurity issues.
c) **Data Protection Act**[8] – After the withdrawal of the *Data Protection Bill, 2019*, the government indicated that said Bill was being reworked comprehensively and was tabled before parliament in August 2023. It was then reintroduced as the Digital Personal Data Protection Act, 2023, which has been swiftly enacted by the Indian government.
d) **Proposed Digital India Act**[9] – As part of the larger overhaul and streamlining of the legal architecture applicable to the information technology industry as a whole, the Digital India Act[10] has been proposed to harmonise existing laws, regulate emerging technologies such as AI, and incorporate industry input on blockchain and Web 3.0 regulations to protect digital citizens.

These impending pieces of legislation would need be kept in mind by any Web3, blockchain or cryptocurrency business when operating in India.

Law surrounding Exchanges

Exchanges are the gateway for most retail VDA investors, creators, and enthusiasts to interact with the global VDA markets and ecosystem. They act as vital on- and off-ramps and, as such, tend to interact with a large number of entities, regulators, and businesses. Some key developments in law and enforcement that have impacted how Exchanges conduct business are as follows:

a) the term "Exchange" is now defined as "…*any person that operates an application or platform for transferring of VDAs, which matches buy and sell trades and executes the same on its application or platform*", as per a circular[11] issued by the Central Board of Direct Taxes ("**CBDT**");
b) the new tax regime for VDAs places certain obligations on Exchanges, which will now need to comply with a number of taxation provisions as specified in the IT Act, government notifications and CBDT circulars. The taxation regime pertaining to Exchanges is discussed elaborately in the "Taxation" section of this chapter; and

c) over the past year, some Exchanges have been investigated for allegedly assisting foreign firms in laundering their money via private cryptocurrencies.[12] The cross-border transactions, taking place through Exchanges, are being heavily scrutinised by authorities such as the ED.

Cryptocurrency regulation

VDAs as legal tender

In the current legal landscape, VDAs in India are not expressly regulated nor prohibited. Individuals and entities are allowed to hold, invest in, and transact VDAs, as long as they abide by existing laws. Banks and other RBI-regulated entities must adhere to established due diligence processes in compliance with financial services regulations. However, the government does not recognise cryptocurrencies as legal tender or coin and intends to curb their use in financing illegitimate activities or within the payment system.

In this scenario, it is important to reference the 2020 Supreme Court of India judgment, which acknowledged the dual nature of VDAs: they are not recognised as legal tender, but they can perform many functions of real currency. This judgment underlines the evolving global understanding of VDAs, pointing towards the necessity of developing suitable regulatory mechanisms.[13]

Sales regulation

In the absence of specific law, pieces of legacy legislation that deal with subjects like: (i) trading and issuance of securities; (ii) trading of commodities; (iii) acquisition and sale of assets to and from persons resident outside India; and (iv) acceptance of deposits by companies, are triggered in certain circumstances. The nature of VDAs and their features will determine the regulatory mechanism that will be applicable to them, based on their use case, which will determine whether they will be treated as VDAs or not.

If a VDA is used as a "store of value", e.g. Bitcoin, then it is freely tradable by individuals within India without any reporting requirements apart from the application of the IT Act. Companies incorporated in India, on the other hand, are required to report any VDA holdings to the regulator as part of their annual returns. VDAs may come to be seen as commodities or assets that, if traded by an Indian resident outside of India, would attract exchange control norms notified under the Foreign Exchange Management Act, 1999 ("**FEMA**").

Where VDAs are issued by incorporated entities in India and such VDAs carry rights in the ownership or assets of such entities, such entities may be subject to rules regarding the issue of securities, collective investment schemes and other similar rules and regulations. Similarly, incorporated entities issuing tokens that are akin to deposits being accepted from the public would be subject to rules issued in this regard.

On 23rd February 2022, the Advertising Standards Council of India framed guidelines for the advertising and promotion of VDAs.[14] The salient features of these guidelines are as follows:

a) Advertisements pertaining to VDAs must carry the prescribed disclaimer.
b) Words like "currency", "securities", "custodian" and "depositories" must not be used.
c) Depiction of minors is prohibited.
d) Risks should not be downplayed. VDAs should not be compared to any other regulated assets.
e) Celebrities and influencers are required to carry out proper due diligence before taking part in such promotions.[15]

Furthermore, after the enactment of the Finance Act, 2022, trading of VDAs is subject to taxation as discussed below.

Taxation

Income from the trade of VDAs is taxable in India, both direct (income tax) and indirect (GST) taxation.

Income tax

The Finance Act, 2022, additional government notifications, and guidelines framed by the CBDT have brought VDAs under the tax regime. These changes can be summarised as follows:

1) **Definition of VDAs**: The definition of VDAs has been kept broad and the government has reserved the right to notify new kinds of digital assets. Further, the government has excluded the following from the definition of VDAs: (a) gift cards or vouchers; (b) mileage points, reward points or loyalty cards; and (c) subscription to websites, platforms or applications.[16] The definition appears to cover both digital assets as a "currency" through the use of phrases such as "inherent value" and "unit of account", as well as digital assets as an "asset". NFTs have also been included within the ambit of VDAs. As per another government notification,[17] "NFT", for the purpose of income tax, has been defined as "*a token which qualifies to be a virtual digital asset as non-fungible token within the meaning of sub-clause (a) of clause (47A) of section 2 of the Act but shall not include a non-fungible token whose transfer results in transfer of ownership of underlying tangible asset and the transfer of ownership of such underlying tangible asset is legally enforceable*".
2) **Tax on income from VDAs**: A 30% tax on income from the transfer of a VDA is now applicable, which tax shall be in addition to the income tax payable on all other income of the assessee. Apart from the cost of acquisition of the VDA, no other deduction is permissible. Even losses incurred in such trade cannot be set off against taxable income.
3) **Payment on transfer of VDAs**: The purchaser of a VDA is liable to deduct and deposit a withholding tax of 1% of the consideration amount. Where the consideration is in kind, wholly or partially (and the cash component is not sufficient to meet the threshold for deduction), the consideration shall not be released until tax on the complete consideration has been paid. Exemptions and thresholds have been defined for the benefit of certain categories, including individuals.
4) **Gift of VDAs**: Receipt of VDAs by an individual for no consideration or for a price that is at least INR 50,000/- (approx. USD 625) less than fair market value will be considered "income from other sources" in the hands of the recipient.
5) **Guidelines for Exchanges**:[18] A summary of the guidelines applicable to Exchanges is as follows:
    a) The responsibility for withholding tax has been clarified via two scenarios:
        i) Where the Exchange does not own the VDA being transferred, it shall deduct withholding tax. In cases where the Exchange is supposed to credit the broker (who does not own the VDA), both the Exchange and broker need to deduct withholding tax, unless there is an agreement in the alternative between the parties. This will require the Exchange to furnish quarterly statements for such transactions to the authorities.
        ii) Where the Exchange owns the VDA being transferred, the buyer is required to deduct the withholding tax unless there is an agreement in the alternative between the parties.

b) Considering practical difficulties faced by Exchanges when the consideration is in kind or in exchange of another VDA, tax may be deducted by the Exchange itself. Such an alternative mechanism can be implemented based on written agreements with buyers and sellers. In cases where the tax amount deducted is also in kind and needs to be converted into cash, the Exchange will have to adopt other mechanisms as laid down in the circular.

c) The tax required to be withheld shall be on the "net" consideration after deducting GST/charges levied by the Exchange for rendering services.

d) In cases where payment gateways are involved, the gateway will not have to pay tax if the tax has already been deducted by the buyer.

6) **Guidelines for P2P transactions**:[19] For all transactions other than those via Exchanges, the following guidelines are relevant:
   a) When consideration is other than in kind, the buyer is vested with the responsibility to deduct and deposit withholding tax along with several other forms of compliance, like furnishing quarterly statements and so forth.
   b) When consideration is in kind or in exchange of VDA, the buyer will release the consideration in kind after the seller provides proof of payment of such tax.
7) **On mining**: Infrastructure costs incurred in the mining of VDAs will not be treated as cost of acquisition, as the same will be in the nature of capital expenditure, which is not allowable as deductions from taxable income.

GST

The sale of goods in India is subject to GST at specified rates pertaining to the type of goods sold. Should VDAs be classified as "goods", each transaction would attract GST. A seller is typically required to charge the buyer/service recipient the prescribed GST and deposit the same with the authorities. Presently, the service fee being collected by Exchanges is being subjected to an assessment for GST.

There remains, of course, the matter of cross-border VDA transactions and the related interplay between withholding tax and Double Taxation Avoidance Agreements. The movement of VDAs across borders, to and from wallets and exchanges poses an unresolved legal challenge on how to accurately tax the sale of VDAs internationally.

Money transmission laws and anti-money laundering requirements

Currently, the regulation of VDAs in India primarily comes from RBI circulars that mandate checks by entities under its regulation. These regulated entities, despite the pseudonymous nature of VDA transactions, were originally ring-fenced from providing services to crypto businesses due to RBI's efforts to effectively prohibit dealing in VDAs.

However, this was later overturned by the Supreme Court of India. The ruling was replaced by a circular permitting regulated entities to handle VDAs, as long as they conformed with the existing KYC, AML, and Countering the Financing of Terrorism ("**CFT**") requirements. Currently, the ED is actively prosecuting alleged cases of money laundering involving VDAs.

Moreover, certain amendments (discussed above) have broadened the scope of the PMLA to cover various aspects related to VDAs. These include exchange between VDAs and fiat currencies, exchange among different forms of VDAs, transfer of VDAs, safekeeping or administration of VDAs, and engagement in financial services related to an issuer's offer and sale of a VDA. This expansion not only covers transactional aspects but also emphasises the regulatory oversight on participation in and provision of VDA-related financial services.

This is in addition to directions issued by CERT-In[20] stating that "virtual asset service providers", "virtual asset exchange providers" and "custodian wallet providers" must maintain KYC and records of financial transactions for a period of five years.

Promotion and testing

On 13th August 2019, RBI issued the *Enabling Framework for Regulatory Sandbox* ("**Framework**")[21] to promote the adoption and implementation of new technologies in the fintech space in India. The Framework currently includes "*Applications under block chain technologies*", but specifically excludes "*Crypto currency/Crypto assets services; Trading/ investing/settling in crypto assets; Initial Coin Offerings, etc.*" from the purview of the Regulatory Sandbox.

In an updated version of this Framework published on 8th October 2021,[22] the limitations remained consistent. The Second Cohort[23] of this Regulatory Sandbox included a blockchain-based cross-border payment system that sought to leverage the current infrastructure and ensure frictionless and tamperproof monitoring capabilities. Similarly, the Third Cohort of this Regulatory Sandbox included a private limited company that was working on a blockchain-based product that acts as middleware in the blockchain stack, enabling co-lending for the micro, small and medium enterprises sector.[24]

The state of Telangana has pioneered the launch of India's first Web3 Regulatory Sandbox.[25] This initiative provides a controlled environment for selected blockchain startups to test their innovations, addressing the existing gap in clarity and support for blockchain and crypto products in the country. The Sandbox facilitates mentorship, regulatory compliance, collaboration with key stakeholders, and market access for startups. It also engages central institutions like the Securities and Exchange Board of India ("**SEBI**"), RBI, and the Insurance Regulatory and Development Authority, enabling them to cooperate with Web3 startups and assess the impact of their solutions.

The inaugural cohort of the Sandbox comprises eight Web3 startups from diverse sectors like finance and social media. Each startup's testing phase is capped at six months in the Sandbox's continuous operating model. Findings and observations on regulatory policies within the Sandbox will be communicated to regulatory bodies and utilised to draft state-level policies. This sandbox initiative is part of Telangana's larger emerging technologies strategy, which includes its blockchain framework and various use cases like e-voting and seed traceability. Collaborating with several Web3 industry players, including the India Blockchain Forum and Sino Global Capital, the Sandbox is a significant step towards the state's ambitious digital innovation goals.

Ownership and licensing requirements

The activities of investment advisors and fund managers are subject to licensing and are governed by SEBI though the SEBI (Investment Advisers) Regulation, 2013 and SEBI (Portfolio Managers) Regulation, 2019.

While there is no specific restriction in the said regulations on advising on and managing VDAs, the list of commodities that managers and advisers can deal in has been notified by SEBI[26] and does not include VDAs. Therefore, any investment advisers or fund managers currently providing services related to VDAs in India are doing so in their personal capacity and not as advisers or managers licensed by SEBI.

Mining

The mining of VDAs is neither prohibited nor regulated in India. As already discussed, costs incurred in the mining of VDAs will be treated as capital expenditure and will not qualify for deduction under the IT Act.

A commercial VDA mining operation in India would be subject to all applicable statutory laws and licensing conditions required for operating any commercial venture, including but not limited to corporate commercial laws, information technology laws, land zoning laws, trade licence, labour licence, etc.

Border restrictions and declaration

RBI is the financial regulator for the nation. It issues exchange and capital control regulations from time to time under FEMA, more specifically:

i) the Foreign Exchange Management (Permissible Capital Account Transactions) Regulations, 2000, which deal with the acquisition and sale of assets situated outside India; and
ii) the Foreign Exchange Management (Export of Goods and Services) Regulations, 2015, which deal with the export of goods (which term includes software) from India *in lieu* of foreign exchange.

Based on the categorisation of VDAs under Indian law as either a capital asset or good, the applicable legislation may be triggered. This would require each cross-border transaction in VDAs to be carried out via authorised dealer banks and be subject to reporting requirements, KYC and other AML protocols.

Reporting requirements

Presently, the Indian government does not require persons to report their VDA transactions except in two circumstances: firstly, reporting of any income or profits from VDA in the income tax returns; and secondly, as required by the Companies Act, 2013.

In addition to this, the MeitY put out a circular mandating all virtual asset service providers, virtual asset exchange providers and custodian wallet providers (as defined by the Ministry of Finance from time to time) to maintain KYC/AML data of its users. This makes it easier for authorities to trace large transactions in the future. P2P sales, however, remain unchecked except to the extent that all transaction details are required to be reported to the tax authorities for the purposes of the IT Act.

Reporting under the PMLA

The PMLA Notification brings all crypto businesses (including exchanges, custodians and wallet providers) under the purview of the PMLA and Rules. This has expanded the meaning of Reporting Entities under the PMLA. "Reporting Entity" is defined under section 2(1)(wa) of the PMLA as "*a banking company, financial institution, intermediary or a person carrying on a designated business or profession*". The PMLA and Rules specify that every Reporting Entity shall mandatorily comply with its directions, including: (a) verifying the identity of clients; (b) conducting due diligence; (c) recording and monitoring transactions; (d) timely reporting of transactions; (e) retention of records for a specific period of time; and (f) maintaining confidentiality.

Under section 12 of the PMLA, every Reporting Entity is mandated to maintain a record of all transactions and documents evidencing the identity of clients and furnish the same to the central government, including furnishing information and reporting suspicious transactions

to the Financial Intelligence Unit, Government of India ("**FIU-IND**"). In addition, under Rule 5(2) of the Rules, every Reporting Entity must develop an internal mechanism for maintaining such information.

The FIU-IND has further issued the *AML & CFT Guidelines for Reporting Entities providing services related to Virtual Digital Assets* ("**Guidelines**"), which are specifically applicable to service providers in the cryptoasset (VDA) space. Though the Guidelines do not have the force of law and have only been issued as a guide to the obligations under the PMLA and Rules, the Guidelines do encapsulate some of the recommended best practices that ought to be followed by entities providing services related to cryptoassets/VDAs.

Estate planning and testamentary succession

There are no specific laws or regulations regarding the treatment of VDAs for the purposes of estate planning or testamentary succession. Individuals in India are bound by their personal laws *viz*. succession. Depending on the individual, the applicable personal laws would be the Hindu Succession Act, 1956, the Indian Succession Act, 1925, or the Muslim Personal Law (Shariat) Application Act, 1937, or in cases where a will has been executed by an individual who follows the Islamic faith, the succession will be governed under the relevant Muslim personal law, which is not codified.

The first aspect to consider is how the right will devolve from the owner of VDAs to his intended beneficiaries. This right may flow through a will, or through operation of law in the event that the owner of the assets dies intestate.

The second aspect to consider is the manner in which the right to the VDAs devolves upon the beneficiaries. The primary challenge, as it exists today, is to enforce and/or exercise the right bequeathed to a beneficiary over VDAs.

In case of wills, to ensure that beneficiaries receive all VDAs left behind by the testator, the testator will need to put a mechanism in place enabling their executor(s) to take charge of and transfer VDAs to the intended beneficiaries.

Regardless of the mode of devolution of the right on the beneficiary, novel solutions may have to be devised to ensure delivery of e-wallets or private keys to beneficiaries. Smart contracts may play an important role in arriving at such solutions. A positive development in this regard is the recent amendments to the IT Act, where the definition of "property" has been expanded to include VDAs, thus attaching all legacy statutes to VDAs and reducing any potential friction.

* * *

Endnotes

1. https://www.meity.gov.in/writereaddata/files/National_BCT_Strategy.pdf
2. https://rbi.org.in/scripts/PublicationReportDetails.aspx?ID=1239
3. https://www.indiabudget.gov.in/doc/Finance_Bill.pdf
4. https://www.rbi.org.in/Scripts/BS_PressReleaseDisplay.aspx?prid=54187
5. https://sansad.in/getFile/loksabhaquestions/annex/1712/AU587.pdf?source=pqals
6. https://www.meity.gov.in/writereaddata/files/National%20Data%20Governance%20Framework%20Policy_26%20May%202022.pdf
7. https://pqars.nic.in/annex/256/AU3439.pdf

8. https://www.theweek.in/news/india/2022/09/06/govt-to-make-online-world-more-accountable--vaishnaw.html
9. https://www.thequint.com/tech-and-auto/tech-news/india-is-moving-to-replace-decades-old-it-act-with-new-digital-india-act-and-data-governance-framework-rajeev-chandrasekar#read-more
10. https://www.thehindubusinessline.com/info-tech/draft-digital-india-act-will-regulate-emerging-technologies-to-protect-citizens-rajeev-chandrasekhar/article66960829.ece
11. https://incometaxindia.gov.in/communications/circular/circular-no-13-2022.pdf
12. https://www.coindesk.com/policy/2022/08/11/indias-ed-probes-at-least-10-crypto-exchanges-on-money-laundering-allegations-report
13. https://main.sci.gov.in/supremecourt/2018/19230/19230_2018_4_1501_21151_Judgement_04-Mar-2020.pdf
14. https://www.ascionline.in/wp-content/uploads/2022/09/vda-guidelines-press-release-feb-23.pdf
15. https://www.coindesk.com/policy/2022/06/29/influencers-are-responsible-for-92-of-crypto-ad-violations-in-india-report-says
16. https://www.indiabudget.gov.in/doc/Finance_Bill.pdf
17. https://incometaxindia.gov.in/Communications/Notification/Notification-No-75-2022.pdf
18. https://incometaxindia.gov.in/communications/circular/circular-no-13-2022.pdf
19. https://www.pdicai.org/Docs/circular-14-2022_296202213596419.pdf
20. https://www.cert-in.org.in/PDF/CERT-In_Directions_70B_28.04.2022.pdf
21. https://rbidocs.rbi.org.in/rdocs/PublicationReport/Pdfs/ENABLING79D8EBD31FED47A0BE21158C337123BF.PDF
22. https://rbi.org.in/scripts/PublicationReportDetails.aspx?ID=1187
23. https://rbi.org.in/scripts/BS_PressReleaseDisplay.aspx?prid=54057
24. https://rbi.org.in/scripts/BS_PressReleaseDisplay.aspx?prid=53813
25. https://web3sandbox.telangana.gov.in
26. Section 2(bc) of the Securities Contracts Regulation Act, 1956 and https://www.sebi.gov.in/legal/circulars/sep-2016/list-of-commodities-notified-under-scra_33359.html

* * *

Acknowledgment

The authors acknowledge with thanks the valuable contribution of Mr. Sanchith Shivakumar to this chapter.

Nishchal Anand
Tel: +91 98 9912 1634 / Email: nishchal@legalpanda.in

Nishchal is an intellectual property and technology law attorney who has been practising in New Delhi since 2009. Besides representing large corporations in contentious IP and data protection matters, he regularly advises tech companies and startups on legal and regulatory compliance including IP structuring, product structuring and data compliance. Nishchal has been part of many landmark judgments furthering the jurisprudence on IP and data protection laws in India. He regularly advises clients across industries on the application and commercialisation of cutting-edge technologies such as blockchain, AI, UAVs, extended reality, and CRISPR. Nishchal has a robust media and entertainment law practice.

Pranay Agrawala
Tel: +91 99 5390 6994 / Email: pranay@legalpanda.in

Pranay is a partner at Panda Law and a technology lawyer who has been practising corporate and commercial law since 2009. He specialises in understanding technologies and bridging the gap between law and tech. He represents clients in the infrastructure, recycling, software & ITES, cryptocurrency, blockchain and allied industries, advising on commercial contracts and M&A transactions as well as appearing before arbitral tribunals and judicial authorities. He regularly advises multinational companies and startups on structuring, incorporation, employment, regulatory and fundraising matters. Pranay has also had the privilege of representing the Union of India before the Supreme Court of India, and presently represents government departments and public sector companies before High Courts and District Courts.

Dhrupad Das
Tel: +91 98 1166 0845 / Email: dhrupad@legalpanda.in

Dhrupad is a partner at Panda Law and has been practising as a litigator in Delhi and Guwahati for over 12 years. His technology practice is focused on cryptocurrency and blockchain regulation, structuring of novel digital assets and tokens, and the integration of emerging technologies with traditional legal and business models, and his traditional practice is focused on corporate dispute resolution, securities laws, corporate insolvency and resolution, competition law, and banking law. He also regularly advises and represents publicly listed companies, public sector enterprises, regulatory bodies and entities in the blockchain and cryptocurrency industry.
Dhrupad is an NFT artist and holds a Permaculture Design Certificate.

Panda Law

A-4, Second Floor, Pamposh Enclave, New Delhi – 110048, India
Tel: +91 11 4102 3333 / URL: www.legalpanda.in

Ireland

Keith Waine, Karen Jennings & David Lawless
Dillon Eustace LLP

Government attitude

The Irish Government has been keen to demonstrate its support of the development and adoption of new technologies, including blockchain, as a way to encourage digitalisation and foster innovation. In a paper issued in December 2019 entitled "International Financial Services Strategy 2025" (**IFS2025**), the Government stated its commitment to developing Ireland as a global leader in the financial services sector and announced measures aimed at demonstrating Ireland's credentials as an EU centre of excellence for distributed ledger technology (**DLT**).

The Government established the Fintech Steering Group in 2021 and, under its "Action Plan for 2022", launched under the IFS2025, it plans to implement the second phase of the Fintech Steering Group. The Steering Group will continue to assist in developing Ireland's policy, consult with industry and key stakeholders from the sector, conduct research and contribute to EU policies. In addition, a working group will be established that will include Steering Group members as well as representatives from the financial services, information technologies and academic disciplines.

The Government is also committed to developing a programme of international activities to raise the global visibility of Ireland as a centre for fintech. Under this initiative, the Department of Finance will work with selected embassies, diplomatic and trade missions abroad, and the enterprise agencies to prepare its focused programme of international activities. Its aim is to increase awareness of Ireland's fintech sector, grow exports for Irish fintech firms and encourage multinational firms to consider Ireland as a location for their fintech activities.

Since June 2018, the Industrial Development Authority (**IDA**), a semi-state body with a mandate to attract foreign direct investment into Ireland, has worked with the Irish Blockchain Expert Group on the "Blockchain Ireland" initiative. This forum is led by the IDA and seeks to enhance the blockchain industry in Ireland and to promote Ireland as a blockchain centre of excellence.

However, the Irish Government has so far been reticent in issuing firm guidance concerning its policy towards DLT and the treatment of virtual currencies from a legal and regulatory perspective.

In March 2018, the Department of Finance issued a discussion paper on Virtual Currencies and Blockchain Technology, with the general aim of describing the current environment, providing an overview of the global virtual currencies market and providing an overview of the potential risks and benefits of virtual currencies. On foot of this paper, an intra-departmental working group was established in 2018 in order to oversee developments in virtual currencies and blockchain technology and consider whether policy recommendations are required. No such policy recommendations have been issued to date.

The Central Bank of Ireland (**Central Bank**), as the authority responsible for the regulation of financial services in Ireland, has led the way in setting policy in this area and has issued a number of consumer warnings on the risks of buying or investing in virtual currencies and initial coin offerings (**ICOs**).

In February 2018, consumers were warned by the Central Bank about the risks of buying or investing in "virtual currencies" and cryptocurrencies,[1] with the Central Bank highlighting risks such as extreme price volatility and the absence of regulation. In 2021, the Central Bank updated the warning to state that, despite the introduction of a new anti-money laundering (**AML**) and countering the financing of terrorism (**CFT**) supervisory regime for certain virtual currency exchanges and custodian wallet providers, this does not change the fact that virtual currencies are not currently regulated, and consumers remain exposed to the risks highlighted in the 2018 warning.

Similarly, the Central Bank sought to alert consumers to the high risks associated with ICOs, such as vulnerability to fraud or illicit activities, lack of exit options, extreme price volatility, inadequate information and exposure to flaws in the technology.[2] It has also indicated its support of the warnings published by the European Securities and Markets Authority (**ESMA**) concerning the risks of ICOs and crypto-assets[3] whereby ESMA underlined the risks that unregulated crypto-assets pose to investor protection and market integrity. ESMA identified the most significant risks as fraud, cyber-attacks, money laundering and market manipulation.

The most recent warning on cryptocurrencies was issued by the Central Bank in March 2022 as part of a European-wide campaign by the European Supervisory Authorities.[4]

Crypto-assets (including cryptocurrencies) are not considered money or equivalent to fiat currency in Ireland and there are currently no cryptocurrencies that are backed by either the Irish Government or the Central Bank.

As discussed below, Ireland has transposed the EU's Fifth Money Laundering Directive (Directive 2018/843/EU) (**MLD5**) into Irish law, which extends AML/CFT requirements to cover certain virtual currency exchanges and custodian wallet providers.

Cryptocurrency regulation

Although the Central Bank has issued warnings in relation to investment in crypto-assets, there is currently no prohibition or ban on cryptocurrencies in Ireland. However, Ireland has not implemented a bespoke financial regulatory regime for cryptocurrencies and there are currently no plans to do so at a local level.

The question of whether and how crypto-assets are regulated under Irish law turns primarily on whether activities carried on in relation to those crypto-assets are regulated under existing legislation in Ireland, which implements certain EU Single Market Directives, such as the Markets in Financial Instruments Directive 2014/65/EU (**MiFID**), the Electronic Money Directive 2009/110/EU (**E-Money Directive**) and the Payment Services Directive 2015/2366/EU (**PSD2**), and by various EU regulations, such as the Prospectus Regulation 2017/1129/EU, the Market Abuse Regulation 506/2014/EU and the Central Securities Depositories Regulation 909/2014/EU, which have direct effect in Ireland.

The Central Bank has indicated its hesitancy towards issuing new domestic legislation to regulate crypto-assets and cryptocurrencies. In 2018, Gerry Cross, Director of Financial Regulation – Policy and Risk at the Central Bank, indicated that:

> "*... it can be easy, when faced with a new and challenging issue or activity, for a regulator to say that A or B is very risky, or that X or Y can have harmful effects and to start in straightaway to consider how to restrict them, regulate them or even*

> *ban them. ... However it is important, in whatever we are looking at, that we take a considered approach; that we think about the potential benefits, including longer term benefits, as well as risks. We need to be clear and precise about what it is we are trying to achieve. We need to reflect on approaches to accomplishing those objectives which retain as much as possible of the potential benefits while addressing the harms, approaches that are in other words proportionate. We also need to think about the potential unforeseen consequence of regulation, including the desirability of giving a "regulatory imprimatur" to the activity in question.*"[5]

As a result, the Central Bank has maintained a "wait and see" approach with regard to implementing domestic regulation, taking guidance from international regulators and most notably European Supervisory Authorities.

On 24 September 2020, the European Commission adopted the Digital Finance Package. This package included a proposal for a Regulation on Markets in Crypto-assets (**MiCA**), in addition to a proposal for a Regulation on digital operational resilience for the financial sector, a proposal on a pilot regime for market infrastructures based on DLT, and a proposal to clarify or amend certain related financial services rules.

MiCA has since been adopted and was published in the Official Journal of the EU as of June 2023.[5] MiCA will apply in its entirety from 30 December 2024, bringing with it the first harmonised rules for crypto-assets in the EU.

MiCA establishes uniform rules for crypto-asset service providers and issuers at EU level, provide measures ensuring consumer and investor protection, and includes safeguards to address potential risks to financial stability.

In a letter to the Minister for Finance from February 2022, Gabriel Makhlouf, the Governor of the Central Bank, stated that "*the significant interest amongst Virtual Asset Service Providers (**VASPs**) in seeking registration with the Central Bank [under the AML/CFT regime (see below)] suggests that interest in authorisation as Crypto Asset Service Providers (**CASPs**) under MiCA will be high*".[6]

The European Banking Authority (**EBA**) has been tasked with developing a number of technical standards and guidelines giving further effect to MiCA. It opened the first consultations in July 2023 on its proposed technical standards for the application for authorisation to offer to the public and to seek admission to trading of asset-referenced tokens (**ARTs**) (a type of "stablecoin") and on complaint handling.[7] In addition, ESMA also opened consultations in July 2023 on seven sets of draft technical standards under MiCA.[8] On 9 August 2023, the Department of Finance opened its consultation on the exercise of national discretions under MiCA.[9] This consultation was due to close on 5 September 2023.

Until MiCA enters into force, cryptocurrency will continue to be unregulated, save where it is subject to regulation under existing financial services regulatory regimes or for AML/CFT purposes.

"Classic" cryptocurrencies (such as Bitcoin, Litecoin and Ether) that are not centrally issued and give no rights or entitlements to holders currently appear to fall outside of the scope of the existing regulatory regime in Ireland. This is on the basis that a pure, decentralised cryptocurrency is unlikely to be a transferable security and the Central Bank has emphasised that such cryptocurrencies are "*unregulated*".[10]

The position is different for that category of cryptocurrencies known as stablecoins – particularly where these coins are pegged to, and are directly exchangeable on demand for, fiat currencies. The Central Bank's 2020 letter indicates that, in its view, "*the risks*

of 'so called stablecoins' for financial stability, monetary policy, consumer and investor protection, legal certainty and compliance with AML/CFT requirements are a key concern. Among the Central Bank of Ireland's key concerns is that the issuing of currency should firmly remain under the remit of the relevant public authorities (i.e. central bank). Where the reach or other features of 'so called stablecoin' risk it being perceived as a currency, or operating as a quasi-currency, then it should be prohibited".

In the context of true utility tokens (i.e. tokens that can be redeemed for access to a specific product or service), the Central Bank indicated in its 2020 letter that "*it is not readily apparent to us that most utility tokens are, or should be, treated as financial products or that they should be regulated as such. However, we recognise that a utility token may, in substance be, or may become, a financial instrument (transferable security or e-money) and, in that case, it should be clear that it should fall within the regulatory perimeter. Cases where crypto assets start as, or claim to be, one thing but morph into the provision of financial services directly or indirectly should be closely monitored*". In the absence of clear Irish or EU legislative guidance, a case-by-case basis analysis is required in order to determine whether a utility token falls outside of the parameters of existing financial services regulation.

In relation to security tokens (which may provide rights such as ownership, repayment of a specific sum of money, or entitlement to a share in future profits), the Central Bank expressed the view in its 2020 letter that it would be beneficial to have a harmonised taxonomy at EU level in relation to crypto-assets, including a harmonised definition of a security token as a transferable security. Hence, where these security tokens are closer to conventional debt instruments and equity instruments, the Central Bank has called for them to be "*consistently regulated, while allowing genuine utility tokens to remain outside the regulatory perimeter*".[11]

Key to any regulatory analysis of security tokens are the concepts of "financial instruments" and "transferable securities" under MiFID. A transferable security for the purposes of MiFID includes shares, bonds, derivatives and other instruments that give their holders similar rights or entitlements. The definition is not exhaustive and includes any security negotiable on the capital market with the exception of instruments of payment. It is clear that a security token may be deemed to be a transferable security for the purposes of MiFID, which would mean that any entity providing an investment service or carrying on an investment activity with respect to the relevant crypto-asset would need to be authorised as an investment firm (and would need to comply with a wide range of detailed prudential and conduct of business requirements), unless it benefits from an exemption.

The DLT Pilot Regime Regulation[12] was published in the Official Journal of the EU on 2 June 2022 with the majority of its provisions applying from 23 March 2023. The pilot regime allows for the trading of certain DLT financial instruments via DLT trading venues and amends the definition of a "financial instrument" in MiFID to clarify beyond any legal doubt that such instruments can be issued via DLT.

Finally, money transmission laws and AML legislation may also apply to activities carried out in relation to cryptocurrencies (see below).

Sales regulation

Where a crypto-asset is deemed to involve an offer of transferable securities to the public, the requirements under the Prospectus Regulation (EU) 2017/1129/EU, as implemented into Irish law by the European Union (Prospectus) Regulations 2019 (together, the **Prospectus Regulations**), may apply.

The Prospectus Regulations impose requirements for an approved prospectus to have been made available to the public before: (a) transferable securities are offered to the public in Ireland; or (b) a request is made for transferable securities to be admitted to a regulated market situated or operating in the EU. Unless an exemption applies (public offers made to certain qualified investors are, for example, exempt), a detailed prospectus containing prescribed content must be drawn up, approved by the Central Bank (or the appropriate EEA Member State financial regulator where Ireland is not the home state of the issuer of the transferable securities) and published before the relevant offer or request is made.

These requirements only apply to offers or requests relating to transferable securities, being anything that falls within the definition of transferable securities in MiFID (see above). In light of the Central Bank's 2020 letter, the Prospectus Regulations would appear to be of primary concern for issuers of security tokens in Ireland.

In addition to the Prospectus Regulations, there are various e-commerce and consumer protection requirements in force in Ireland that are potentially applicable to sales of cryptocurrencies or crypto-assets or the offering of services related to cryptocurrencies or crypto-assets (such as exchange or wallet services) in or from Ireland.

Taxation

There are no specific rules for dealings in crypto-assets or cryptocurrencies; therefore, one has to have regard to the basic principles of Irish tax law. This means that determining the tax treatment of a cryptocurrency transaction requires an assessment of the activities and parties involved, Irish Revenue guidance, case law and relevant legislation. The Irish Revenue confirmed this in a publication issued in May 2018 (which was most recently updated in April 2022).

Whether a supplier of services or goods receives payment of cryptocurrency *in lieu* of cash will not change how that supply is taxed in the hands of the supplier. There is no change to when revenue is recognised or how taxable profits are calculated. As cryptocurrencies are not a functional currency for tax purposes, a company's accounts cannot be prepared in cryptocurrencies for tax purposes. The Irish Revenue notes that while cryptocurrencies are referred to as a currency by many, they are best referred to as assets.

Whether dealing in cryptocurrencies will be treated as a trade of dealing or a capital transaction for taxation purposes will depend on the nature and level of activity of the dealer. Occasional investment in and disposals of cryptocurrencies (the use of cryptocurrencies to purchase goods is seen as a disposal) would likely be treated as a capital receipt, currently taxed at 33%. Where there is significant and regular dealing, this could be considered to be trading, which for a company would be taxed at 12.5%, or the marginal higher rates for individuals. The Irish Revenue notes that a trade in cryptocurrencies would be similar in nature to a trade in shares, securities, or other assets but, while individuals and companies entering into transactions relating to cryptocurrencies may describe the transaction as a "trade", this is not sufficient for it to be regarded as a financial trade for tax purposes. The actual tax position will depend on an analysis of the specifics of each transaction, and would need a case-by-case consideration, as is normal in determining whether a trading activity is being undertaken.

It is acknowledged by the Irish Revenue that the value of cryptocurrencies may vary between exchanges and that there may not always be a single exchange rate for cryptocurrencies. Therefore, a reasonable effort should be made to use an appropriate valuation for the transaction in question. In addition, where there is an underlying tax event involving the use of a cryptocurrency, there is a requirement in tax legislation for a record to be kept of the transaction including any record in respect of the cryptocurrency.

VAT is due in the normal way from suppliers of goods and services sold in exchange for cryptocurrencies. VAT should not arise on the transfer of cryptocurrencies, and income received from cryptocurrency mining activities is considered generally outside the scope of VAT by the Irish Revenue on the basis that the activity does not constitute an economic activity for VAT purposes. Irish stamp duty should not arise, although as stamp duty is a tax on documents, the manner in which the transfer takes place would be worth monitoring to ensure that a stampable document has not been inadvertently created.

The territoriality aspect of cryptocurrencies is still an evolving area. Understanding the source or *situs* of cryptocurrencies is of significance in determining whether a person is subject to Irish tax (in particular non-Irish residents) in cross-border dealings. Generally speaking, an individual who is resident or ordinarily resident in Ireland, but not domiciled in Ireland, is only taxable on foreign income or gains that are remitted into Ireland. The remittance basis applies to assets that are situated outside Ireland, and not to assets that are not situated in Ireland. The Irish Revenue notes the importance of this distinction because, where a cryptocurrency exists "on the cloud", it will not actually be situated anywhere and, therefore, cannot be viewed as situated outside Ireland. Where the *situs* of the cryptocurrency is in dispute, the onus is on the taxpayer to prove where the gain accrued. Where the location of the cryptocurrency giving rise to a taxable gain cannot be confirmed by the taxpayer, that gain is chargeable to tax in Ireland based on residency rules.

Money transmission laws

Money transmission services in Ireland may be subject to the local regulatory regime governing money transmission, but will more likely be subject to the European Communities (Payment Services) Regulations 2018 (the **Payment Services Regulations**) (which implement PSD2 into Irish law). The Payment Services Regulations focus on electronic means of payment rather than cash-only transactions or paper cheque-based transfers. These Regulations may be relevant where a crypto-asset could potentially be considered a payment instrument or if the issuer is operating a payment account. Core concepts of the Payment Services Regulations include "electronic cash" and the transfer of "funds". As neither of these concepts appear relevant in the case of classic cryptocurrencies, or products or ancillary services related thereto, they would appear to fall outside the scope of the Payment Services Regulations.

In the case of crypto-assets other than classic cryptocurrencies or ancillary services, the Payment Services Regulations may be relevant. For example, the operator of a cryptocurrency platform that settles payments of fiat currency between the buyers and sellers of cryptocurrency may be engaged in regulated payment services.

In addition, the European Communities (Electronic Money) Regulations 2011, as amended (the **Irish E-Money Regulations**), which implement the E-Money Directive into Irish law, may be of relevance to certain types of crypto-assets. The Irish E-Money Regulations regulate the issuers of e-money. "Electronic money" is defined as "*electronically (including magnetically) stored monetary value as represented by a claim on the electronic money issuer*". Classic cryptocurrencies would not appear to involve "*a claim on the electronic money issuer*". However, the EBA has indicated that, in certain circumstances, a crypto-asset could qualify as "electronic money",[13] namely where the token is issued on the receipt of fiat currency and is pegged to, and directly exchangeable on demand for, such fiat currency (such as a stablecoin). We would expect the Central Bank to follow this view in Ireland.

Where a particular cryptocurrency qualifies as "electronic money", then an Irish issuer will be required to be authorised under the Irish E-Money Regulations. Such an entity will therefore need to comply with ongoing financial regulatory requirements (some of which are likely to be problematical for certain crypto-assets) and would be subject to AML requirements.

AML requirements

MLD5 requires EU Member States to impose registration and AML requirements on fiat-to-cryptocurrency exchange platforms, as well as custodian wallet providers.

On 23 April 2021, the Criminal Justice (Money Laundering and Terrorist Financing) (Amendment) Act 2021 came into force in Ireland (**Irish Act**). The Irish Act implements MLD5 in Ireland and brings VASPs within the scope of existing AML legislation. VASPs are defined as persons or firms carrying out any of the following activities by way of business on behalf of another:

1. exchange between virtual assets and fiat currencies;
2. exchange between one or more forms of virtual assets;
3. transfer of virtual assets, that is to say, conducting a transaction on behalf of another person that moves a virtual asset from one virtual asset address or account to another;
4. custodian wallet provider, that is to say, providing services to safeguard private cryptographic keys on behalf of customers, to hold, store and transfer virtual currencies; and
5. participation in, and provision of, financial services related to an issuer's offer or sale of a virtual asset or both.

A "virtual asset" is defined as "*a digital representation of value that can be digitally traded or transferred and can be used for payment or investment purposes but does not include digital representations of fiat currencies, securities or other financial assets*".

From 23 April 2021, VASPs established in Ireland are required to register with the Central Bank for AML/CFT purposes. The Central Bank may refuse a registration in circumstances where it is not satisfied with the VASP's AML/CFT policies and procedures, and/or the fitness and probity of the senior management and/or beneficial owners of the VASP. The Central Bank has the power to revoke registrations and to impose any conditions that it considers necessary for the proper and orderly regulation of the business.

VASPs are subject to the same AML/CFT requirements as other financial service providers, including the obligation to conduct an AML/CFT business risk assessment, carry out customer due diligence on their customers, carry out ongoing monitoring of customers and their transactions, and file suspicious transaction reports with the relevant authorities. Once registered, the VASP is required to include a regulatory disclosure statement in the prescribed form in all advertisements for its services, stating that it is regulated by the Central Bank for AML/CFT purposes only.

In July 2022, the Central Bank published an AML Bulletin[14] focusing on the application process for registration as a VASP. Shortly after, it was announced that the Central Bank had registered its first VASP. The AML Bulletin outlines the Central Bank's observations following its assessment of applications for VASP registrations and identifies a number of recurring weaknesses where the Central Bank was not satisfied with the level of information and documentation provided by applicant firms.

Also in the area of AML, the European Commission, in July 2021, published its proposal for a Regulation on information accompanying transfers of funds and certain crypto-assets. On 9 June 2023, the Regulation[15] was published in the Official Journal of the EU, bringing

the traceability requirements for transfers of fiat funds to transfers of crypto-assets (the so-called "**Travel Rule**"). The Travel Rule will apply from 30 December 2024, aligning with the application of MiCA.

Promotion and testing

In April 2018, the Central Bank launched its Innovation Hub, designed to facilitate open and active engagement with the fintech sector. The Central Bank has stated that:

> "*This was done with three aims in mind: firstly, to provide us with a way to engage more effectively with persons and entities engaged in fintech innovation, so that we as supervisors could gain an enhanced understanding of the developments underway and likely to emerge. Secondly to enhance our discussions on regulatory aspects with innovators, for many of whom the world of financial regulation is an unaccustomed and potentially intimidating one. And thirdly, to help ensure that new financial firms emerging onto the market are well placed to comply with the requirements of financial regulation which is key to the continuing achievement of the consumer protection and financial stability outcomes that are at the heart of our mandate*."

However, to date, Ireland has not established a regulatory sandbox to allow firms to test innovative financial services propositions in the market with real consumers.

The DLT Pilot Regime Regulation allows for the controlled trading of DLT financial instruments and provides for derogations from existing rules that are not consistent with DLT technology. The pilot regime will allow companies to learn more about how existing rules fare in practice.

Ownership and licensing requirements

There are no specific prohibitions in Irish law on the ownership or control of crypto-assets. However, the nature and form of property rights that may exist in relation to crypto-assets under Irish law is currently untested.

As to licensing requirements, whether or not a person requires authorisation to perform their activities in relation to crypto-assets in Ireland will depend on a case-by-case analysis of the activities to be performed and the nature of the crypto-asset itself. It will also involve a case-by-case analysis of the various securities laws in Ireland arising under both EU and domestic legislation as detailed above under the headings "Cryptocurrency regulation", "Sales regulation" and "Money transmission laws and anti-money laundering requirements". As in many jurisdictions, the regulatory environment in Ireland in relation to cryptocurrencies and their interaction with securities law is not yet settled.

Certain products, such as UCITS funds, which are intended to be marketed to retail investors in the EU, are subject to specific restrictions on the type and diversity of assets they can hold. The Central Bank confirmed in April 2021 that it "*is highly unlikely to approve a UCITS proposing any exposure (either direct or indirect) to crypto assets*".[16] However, the Commission is planning a wide-ranging review[17] of UCITS rules governing eligible investments as set out under the Eligible Assets Directive.[18] As part of that review, ESMA has been asked to consider whether exposure to crypto-assets could lead to divergent interpretations and/or risks for retail investors. ESMA is requested to deliver its technical advice by 31 October 2024.

The ability for Irish regulated funds, other than UCITS, to invest in crypto-assets has recently been clarified by the Central Bank. In April 2023, the Central Bank published its

updated Q&A on digital assets,[19] which confirmed that, in principle, indirect investment in digital assets is permitted by Irish alternative investment funds that are marketed to investors (other than retail investors) subject to applicable conditions being met.

Finally, certain crypto-assets (such as stablecoins) could potentially be categorised as an alternative investment fund in certain limited circumstances (such as where the value is pegged to the performance of a pool of underlying assets), giving rise to licensing requirements relating to the issue, operation and marketing of the fund and its service providers.

Mining

There are no specific restrictions on the mining of Bitcoin or other cryptocurrencies in Ireland. However, the Central Bank has been keen to highlight the potential negative environmental impacts of virtual currency mining.[20] Concern regarding the environmental impact of virtual currency mining is especially relevant due to the recent focus of EU institutions on sustainable finance and the publication of the European Commission's Sustainable Finance Action Plan.

Border restrictions and declaration

There are no specific border restrictions or declarations that must be made on the ownership of cryptocurrencies in Ireland. Individuals carrying cash in excess of EUR 10,000 must declare this to the Revenue Commissioners on entering Ireland from a country outside the EU. However, as cryptocurrencies are not regarded as cash in Ireland, this requirement does not apply to cryptocurrencies.

Reporting requirements

Currently, there are no specific reporting requirements in place for crypto-assets in Ireland. However, any transactions should be monitored to ensure that they are compliant with AML and CFT procedures, particularly in light of the implementation of MLD5 in Ireland (see above).

Estate planning and testamentary succession

There is no explicit legislation in Ireland addressing the treatment of crypto-assets in the context of estate planning and testamentary succession. In principle, it is expected that any crypto-assets or crypto-assets accounts would be treated as personal property and would fall into the estate of the deceased, which can be administered by the executor (in the case of a will) or an administrator (in the case of intestacy).

* * *

Endnotes

1. https://www.centralbank.ie/consumer-hub/consumer-notices/consumer-warning-on-virtual-currencies (updated April 2021).
2. https://centralbank.ie/consumer-hub/consumer-notices/alert-on-initial-coin-offerings
3. ESMA, Advice on Initial Coin Offerings and Crypto-Assets, 2019.
4. https://www.centralbank.ie/news-media/press-releases/central-bank-warning-on-investing-in-crypto-assets-22-march-2022#:~:text=The%20Central%20Bank%20has%20today,be%20suitable%20for%20retail%20customers

5. Regulation (EU) 2023/1114 of the European Parliament and of the Council of 31 May 2023 on markets in crypto-assets, and amending Regulations (EU) 1093/2010 and (EU) 1095/2010 and Directives 2013/36/EU and (EU) 2019/1937.
6. "Tomorrow's yesterday: financial regulation and technological change" – speech given by Gerry Cross, Director of Financial Regulation – Policy and Risk, Central Bank of Ireland, at Joint Session: Banknotes/Identity High Meeting 2018.
7. EBA Consultation Paper of 12 July 2023 (EBA/CP/2023/15) entitled "Draft Regulatory Technical Standards on information for application for authorisation to offer to the public and to seek admission to trading of asset-referenced tokens and Draft Implementing Technical Standards on standard forms, templates and procedures for the information to be included in the application, under Article 18(6) and (7) of Regulation (EU) 2023/1114".
8. ESMA Consultation Paper of 12 July 2023 entitled "Technical Standards specifying certain requirements of the Markets in Crypto Assets Regulation (MiCA)".
9. Department of Finance Public Consultation entitled "Markets in Crypto Assets Regulation ((EU) 2023/1114).
10. https://www.centralbank.ie/consumer-hub/consumer-notices/consumer-warning-on-virtual-currencies (updated April 2021).
11. Speech at Digital Finance in Europe by Gerry Cross, Director of Financial Regulation – Policy and Risk, Central Bank of Ireland on 14 May 2020.
12. Regulation (EU) 2022/858 of the European Parliament and of the Council of 30 May 2022 on a pilot regime for market infrastructures based on distributed ledger technology, and amending Regulations (EU) 600/2014 and (EU) 909/2014 and Directive 2014/65/EU.
13. See Box 3 on page 13 of the EBA's Report of 9 January 2019 entitled "Report with Advice for the European Commission".
14. Central Bank Anti-Money Laundering Bulletin, Issue 8, July 2022.
15. Regulation (EU) 2023/1113 of the European Parliament and of the Council of 31 May 2023 on information accompanying transfers of funds and certain crypto-assets and amending Directive (EU) 2015/849.
16. Central Bank of Ireland's UCITS Q&A, 32nd edition, 29 July 2021.
17. Letter of 16 June 2023 from the European Commission to Ms Verena Ross, the Chair of ESMA, entitled "Formal request to ESMA for technical advice on the review of Commission Directive 2007/16/EC on UCITS eligible assets".
18. Commission Directive 2007/16/EC on UCITS eligible assets.
19. Central Bank of Ireland's AIFMD Q&A, 47th edition, 4 April 2023.
20. Speech at Joint Session: Banknotes/Identity High Meeting by Gerry Cross, Director of Financial Regulation – Policy and Risk, Central Bank of Ireland on 20 March 2018.

Keith Waine
Tel: +353 1 673 1822 / Email: keith.waine@dilloneustace.ie

Keith is Head of the firm's Financial Regulation team and provides regulatory advice to international banks, investment firms, payments firms, non-bank lenders, and other financial services providers.

Keith advises on a range of regulatory matters, including authorisation processes, regulatory perimeter issues, MiFID, individual accountability and consumer protection. He has particular expertise in anti-money laundering (AML) compliance, having previously been Head of Legal and Compliance with responsibility for AML at a full-service Irish bank.

Many of Keith's clients operate in the investments, payments and crypto-assets sectors and he is currently advising a number of firms on applications for authorisation in Ireland.

Prior to joining Dillon Eustace LLP, Keith spent 10 years working in industry in senior executive roles, including as Co-Founder of an alternative mortgage lender.

Karen Jennings
Tel: +353 1 673 1810 / Email: karen.jennings@dilloneustace.ie

Karen is a Senior Associate in the Financial Regulation team. Karen advises clients operating across a wide spectrum of financial services including asset and fund management, banking and payments, credit servicing and insurance. Karen provides advice on Irish authorisation and licensing issues and on regulatory and compliance matters affecting financial firms such as EMIR, AML/CFT requirements, confidential information and data protection requirements, outsourcing, business continuity and disaster recovery. Karen also advises clients on regulatory capital and corporate governance requirements.

David Lawless
Tel: +353 1 673 1765 / Email: david.lawless@dilloneustace.ie

David advises on all taxation aspects of financial services – including structured finance transactions, investment management, capital markets, real estate, private equity, banking, treasury and reinsurance. He established the Dillon Eustace LLP tax practice in 2004 after joining the firm from PwC, where he was a financial services tax partner since 1996. David has written and spoken extensively on tax topics and has participated in public/private tax committees in Ireland focused on making Ireland an attractive tax location. He is a member of the international and VAT tax committees of Irish Funds and the tax committees of the Alternative Investment Management Association, the Irish Debt Securities Association and the Law Society of Ireland.

Dillon Eustace LLP

33 Sir John Rogerson's Quay, Dublin 2, D02 XK09, Ireland
Tel: +353 1 667 0022 / URL: www.dilloneustace.com

Israel

Uri Zichor
FISCHER (FBC & Co.)

Government attitude and definition

The Israeli government broadly supports advances in technology, as well as the regulation of laws and incentives that can further industry growth. The government's general approach towards cryptocurrencies is that there is a need to establish a comprehensive regulatory framework for cryptocurrencies and tokenised securities. Recognising the various implications associated with cryptocurrency activities, including money laundering, potential financial instability, privacy concerns, fraud, and the unique market risks inherent to the crypto industry, the Israeli government acknowledges that the absence of adequate regulation may exacerbate these risks. To address these concerns and the absence of clear guidelines, the government is committed to enacting legislation and implementing an informed risk management structure. By achieving an appropriate regulatory framework, Israel can effectively balance technological innovation and regulatory oversight.

In Israel, cryptocurrencies are not treated as "money" or given otherwise equal status as domestic or foreign fiat currency. In 2018, the Israeli Tax Authority ("**ITA**") issued Circular 5/2018 stating that virtual currencies are considered "assets" and not currency.[1] Therefore, the sale of a digital asset for profit, including the exchange of one asset for another, is subject to a capital gains tax of 25% rather than income tax. This aligns with the provisions set forth in the Supervision of Financial Services (Regulated Financial Services) Law of 2016 ("**Financial Services Law**"),[2] which outlines a list of assets that may fall under the definition of "financial assets", with virtual currencies being included among them.

In Israel, individuals are permitted to exchange cryptocurrency for the local fiat currency (NIS). There are currently no cryptocurrencies that are backed by the Israeli government or a central bank. However, there is a central bank digital currency project for a digital shekel.[3] It is important to note that from the Israeli government's perspective, cryptocurrency is not deemed an acceptable means of payment and is primarily used for financial investment purposes.

Cryptocurrency regulation

Israel has yet to implement a comprehensive legal structure that regulates cryptocurrencies. Nevertheless, multiple regulatory bodies oversee cryptocurrency activities.

Israeli Securities Authority ("**ISA**")

The ISA is one of the most prominent authorities in Israel to address cryptocurrency regulations.

Subcategorising cryptocurrencies

The ISA released two reports discussing the issuance of cryptocurrency and the regulation of public offerings. The first report was an interim report by the Committee for the Regulation

of Public Offerings of Decentralised Cryptocurrency Coins, which was released in March 2018.[4] Building upon the interim report, the finalised report ("**Finalised Report**") was published a year later in 2019, providing further insights.[5] Notably, the Finalised Report introduced three distinct subcategories for cryptocurrencies:

(1) currency tokens – intended to be used as a means of payment;
(2) security tokens – grant a right of ownership or membership participation; and
(3) utility tokens – grant a right to access or use a service or product.

This framework aims to assist decision-makers in the classification of tokens as securities for the purpose of public offerings. The Finalised Report further deduced that tokens will be deemed securities if they do not enable any other right, including a right to profits or participation from a company that is the offeror or issuer of the tokens.

The Finalised Report also differentiated between initial coin offerings ("**ICOs**") and security token offerings ("**STOs**"). The offering of securities to the public falls under the supervision of the ISA. Accordingly, offerings of cryptocurrencies to the public can fall under the definition of a "security".

In 2019, the Finalised Report stated that the classification of tokens as a "security" should be determined via the U.S.'s *Howey* test.[6] Thus, when tokens issued in ICOs are classified as securities, the fundraising is subject to the ISA. If tokens issued in public offerings are classified as utility tokens, then the fundraising is not subject to regulatory requirements other than contractual obligations. According to the Finalised Report, the indicators relevant for the classification of security tokens include:

(1) the purpose of the purchase of the tokens by the purchasers thereof;
(2) the level of functionality of the tokens at the time of their sale; and
(3) the representations and undertakings of the issuer, including promises to yield and creating a secondary market.

The Finalised Report, together with Government Decision No. 204 of February 24, 2023,[7] stipulated additional regulatory bodies in Israel to act with the intention of advancing the "regulation of activity in digital assets". A recent advancement made during May 2023 was the appointment of a team to examine the legal status of decentralised autonomous organisations ("**DAOs**") by the Director General of the Ministry of Finance and the Deputy Legal Advisor to the Government (Economic Law).[8] Presently, within Israel's regulatory regime, DAOs are not recognised as legal entities or limited companies, as there is no provision for beneficial ownership. Consequently, decentralised organisations cannot be registered as corporations or engage with financial institutions or regulatory authorities within Israel. For this reason, the team aims to examine the required regulation, corporate status, taxation aspects, and other aspects of DAOs to create legal certainty, reduce the risk factors in the activity through DAOs and create a better understanding of their potential for the Israeli economy.

Investors in cryptocurrency

In the absence of specific regulations governing cryptocurrency investors, they are subject to regulation by the Israeli Securities Law of 1984,[9] which applies to all investors. Nonetheless, this statute defines "sophisticated investors" as individuals eligible to engage in ICOs without the requirements of a prospectus.

To be a "sophisticated investor", investors must meet one of the following requirements:

(1) their total value of liquid assets owned exceeds NIS 8 million;
(2) their income in the past two years exceeds NIS 1.2 million or the income of the family unit to which they belong exceeds NIS 1.8 million; and

(3) the total value of the liquid assets they own exceeds NIS 5 million and their income in each of the past two years exceeds NIS 600,000 or the income of the family unit to which they belong exceeds NIS 900,000.

Modification of current regulation

In January 2023, the ISA published the "proposal to amend the applicability of securities laws regarding digital assets" ("**Proposal**").[10] The Proposal aims to change the current Securities Law of 1968 ("**Securities Law**").[11] This modification of the Securities Law aims to classify security tokens as "*digital assets designed to serve as an investment in a specific venture, including those that grant similar rights to traditional securities*". When assets are defined as securities, financial assets or financial instruments, as laid out in the Securities Law, then the fundraising is subject to regulatory requirements pursuant to Israeli law.

In the same Proposal, the ISA defined stablecoins as "*assets backed by other assets, whose value is pegged to the value of a commodity or currency through the holding of reserves of the linked assets (or in other assets using algorithms, for the purpose of stabilization) and are intended to be used as means of exchange or payment*". Nonetheless, the classification of stablecoins is still awaiting determination by the ISA and other legislation and regulation in Israel. It is possible that stablecoins will be classified in different ways given their inherent characteristics of no yield and presumably low risk. Still, it is also possible that the classification will vary between fully backed stablecoins and partially backed ones, including "algorithmic" stablecoins that use a formula to maintain their peg. Alternatively, stablecoins might be classified as securities when an issuer is obligated to pay a predefined amount for each token, or as derivatives, if their value is linked to the value of another asset. Moreover, it is possible that the issuance and operation of a stablecoin network will fall under the jurisdiction of the banking services.

The ITA

The ITA is another significant regulatory body that has created guidelines for digital tokens and cryptoassets. In 2017, the ITA issued a statement declaring that the sale of a digital asset is subject to capital gains tax. The ITA classifies cryptocurrencies for tax purposes as "assets", as provided in Article 88 of the Income Tax Ordinance.[12]

Between 2018–2019, the ITA released three circulars that provided further clarification on the taxation of digital assets:

(1) Circular 5/2018 determines that virtual currencies are considered an "asset", and therefore, the sale of a digital asset, including those exchanged for another asset, is subject to a capital gains tax of 25%.[13]
(2) Circular 7/2018 addresses the taxation of utility tokens in ICOs.[14]
(3) Circular 91/2021 explicitly states that the change in the value of Bitcoin is unlike the change that derives from exchange rate differences, which are tax exempt.[15]

Furthermore, in December 2021, the ITA published a "required reporting standpoint" specifying that the exchange of one digital currency for another constitutes a tax event that requires payment and reporting. In March 2022, the ITA published an additional circular clarifying that the sale of non-fungible tokens ("**NFTs**") constitutes a taxable event.

The Bank of Israel

In 2021, the Bank of Israel released a statement directing banks throughout Israel to accept deposits of cryptocurrency when the deposit derives from a corporation that holds a currency trading licence. The objective of this provision was to allow digital currency investors to convert their cryptocurrency to bank accounts utilising approved trading systems.

Consequently, in May 2022, the Israeli Banks Supervisor released the Proper Conduct of Banking Business Directive No. 411 (Prevention of Money Laundering and Financing of Terror, and Customer Identification) ("**Directive**").[16] The Directive outlines guidelines for risk assessment and established policies and procedures for transferring funds involving digital assets utilising a risk-based approach. More importantly, the Directive includes instructions on proper conduct banking and a requirement that establishes clear policies and procedures regarding the provision of payment services in virtual currency. Notably, the Directive regulates and refers specifically to the scenario of funds transferred from the service provider in virtual currency to the client's bank account.

The Capital Market, Insurance and Savings Authority ("**Capital Market Authority**")

In September 2022, the Capital Market Authority published a circular draft concerning the safeguarding of financial assets, including legal tender (fiat) and virtual currencies. The draft determined that service providers must possess the skill and technological means required for safeguarding virtual currencies.

Ministry of Finance

In November 2022, the Chief Economist at the Ministry of Finance published a report with recommendations on the regulation of the digital assets market ("**Report**").[17] The Report covered a wide range of aspects concerning digital assets. In particular, the Report included an overview of the cryptocurrency market in Israel, assessing the risks and specifying the main barriers that prevent proper market development, as well as comprehensive suggestions regarding required regulation and legislation in the field. The recommendations were divided into three main categories:

(1) removing barriers in existing regulation;
(2) improving and expanding on existing regulatory infrastructure; and
(3) creating new regulatory infrastructure.

With the intention of implementing the suggestions of the Report, the ISA published a proposal in January 2023 to amend the Securities Law, meaning that certain definitions will be revised. One prominent change expected to be made is adding a definition for "digital assets", as well as including "digital assets" under possible definitions for "financial instruments".

The Knesset (Israel's unicameral legislature)

In March 2023, the Knesset proposed a new bill with the intention of amending the Income Tax Ordinance (exemption from tax on the sale of digital currencies to non-residents and on the allocation of digital currencies to employees).[18] In July 2023, the bill passed its first reading in the Knesset. It intends to correct the discrimination in taxation suffered by crypto, blockchain and Web3 companies. The bill aims to grant crypto companies the same tax benefits that other Israeli hi-tech companies are entitled to. This will include a tax exemption for foreign investors, so that a foreign resident will be exempt from capital gains tax for the sale of digital currencies and a tax reduction on option grants for employees from 50% to about 25%. Furthermore, the Knesset aims to form a lobby for crypto, blockchain and Web3 with the goal of promoting regulatory certainty in the field.

Sales regulation

An entity that provides financial asset services, including the sale of a "financial asset", requires a financial service provider licence from the Capital Market Authority in accordance with the provisions of the Financial Services Law. Under the Financial Services Law, virtual currency meets the definition of a financial asset.[19] For this reason, crypto-oriented

companies in Israel are required to obtain a service provider licence from the Capital Market Authority. So far, only a few crypto-oriented companies have managed to obtain a licence from the Capital Market Authority, these companies being Hybrid Bridge Holdings Ltd., Bits of Gold, Horizon from Altshuler Shaham and Bit2C.

Furthermore, over the years, the ISA has issued cautionary notices and statements, suggesting that certain cryptocurrencies and token offerings may qualify as securities and therefore be subject to securities regulations.[20] If classified as securities, such digital asset sales and public offerings would be governed by the relevant securities laws in Israel. Additionally, the ITA has classified cryptocurrencies like Bitcoin as "assets", resulting in transactions involving Bitcoin being subject to capital gains tax.

Taxation

The ITA has issued multiple circulars aimed at addressing various aspects related to crypto-currency, including cryptocurrency taxation. These circulars provide regulatory guidance on cryptocurrency taxation, among other related topics.

Circular 5/2018 determines that virtual currencies are considered an "asset"

Circular 5/2018 establishes that virtual currencies, including cryptocurrencies like Bitcoin, are considered "assets" for tax purposes.[21] They are treated as property or investments rather than legal tender. Therefore, the sale of a digital asset, including those exchanged for other assets, is subject to a capital gains tax rate that can range between 25% and 30%, depending on the income level. Circular 5/2018 also states that the exchange of one virtual currency for another is subject to capital gains tax. The tax liability arises from the difference in value between the acquired and disposed virtual currencies at the time of the exchange, yet some of the expenses incurred in the process of acquiring and disposing of cryptocurrencies may be deductible against taxable income. Additionally, if cryptocurrencies are acquired and utilised for business or commercial purposes, any resulting gains or income may be subject to regular income tax rather than capital gains tax.

Circular 7/2018 provides guidance on the taxation of utility tokens in Israel

Circular 7/2018 recognises that utility tokens, which are typically used to access goods or services within a specific platform or ecosystem, serve a functional purpose beyond investment. Accordingly, if utility tokens are acquired solely for personal use or consumption within the platform or ecosystem, they are not subject to capital gains tax. This means that individuals who acquire utility tokens for personal use are not taxed on any potential increase in value. However, if a utility token is acquired for a business or commercial purpose, any gain derived from the disposal or exchange of utility tokens may be subject to taxation as regular business income rather than capital gains. The circular emphasises the importance of maintaining proper documentation and records regarding the acquisition and use of utility tokens, especially for business purposes. It highlights the need for individuals and businesses to accurately report their cryptocurrency activities to the ITA as required by the tax regulations.

Circular 91/2021discusses the conversion of decentralised payments methods[22]

The definition of an "asset" in section 88 of the Income Tax Ordinance includes any property, whether tangible or intangible. "Decentralised means of payment", also referred to as "virtual currency" (such as Bitcoin and Ethereum), is the personal property of the person who owns said virtual currency. Therefore, the ITA classifies digital assets for tax purposes as "assets". For this reason, the sale of cryptocurrencies constitutes a taxable

event according to the provisions of Part E of the Income Tax Ordinance (capital gain). Additionally, cryptocurrencies do not constitute currency or foreign currency as defined in the Bank of Israel Law of 1985. Thus, the difference between the sale proceeds and the purchase cost will not be considered as differentials linkage and/or as rate differentials.

Additional procedures and guidelines regarding the taxation of cryptocurrencies

In December 2021, the ITA published a "required reporting standpoint" by which the exchange of one digital currency for another constitutes a tax event that requires payment and reporting. Then, in March 2022, the ITA published its position stating that the sale of NFTs constitutes a taxable event; this is based on the similar principles published in Circular 5/2018.

More recently, in March 2023, a new bill was proposed by the Knesset with the intention of amending the Income Tax Ordinance (exemption from tax on the sale of digital currencies to non-residents and on the allocation of digital currencies to employees).[23] Please see "The Knesset (Israel's unicameral legislature)" above for more information.

Money transmission laws and anti-money laundering requirements

Under Israeli law, cryptocurrencies are considered a form of "financial asset" and are subject to regulation. The Financial Services Law is the primary legislation that regulates financial service providers, including those dealing with financial assets and virtual currencies.[24] This law requires entities engaged in providing services for the holding, safekeeping, management, transfer, or exchange of financial assets, including cryptocurrencies, to obtain a licence. Cryptocurrency service providers in Israel are required to implement both anti-money laundering ("**AML**") and counter-terrorism financing ("**CTF**") measures. This includes adopting risk-based procedures, customer due diligence measures, ongoing monitoring of transactions, and reporting suspicious activities to the Financial Intelligence Unit ("**FIU**") of the Israel Money Laundering and Terror Financing Prohibition Authority.

In accordance with the provisions outlined in the Financial Services Law and the Prevention of Money Laundering Order (Identification, Reporting and Record Keeping Duties of Providers of Services in Financial Assets and Credit Service Providers for the Prevention of Money Laundering and Terror Financing) of 2018 ("**Money Laundering Order**"), any entity engaged in the provision of services pertaining to the holding, safekeeping, management, transfer or exchange of cryptocurrency is subject to a licensing requirement and AML/CTF duties, including know-your-customer ("**KYC**") duties.[25] The duties require compliance with AML regulations, and cryptocurrency service providers in Israel must perform adequate KYC procedures. This involves verifying the identity of customers, conducting background checks, and obtaining the necessary documentation to verify transactions.

Furthermore, Israeli financial institutions (including banks, insurance companies, pension funds, exchange members, credit providers, providers of services in financial assets, lawyers and certified public accountants) are subject to certain AML obligations and are required to implement a risk-based approach. The AML/KYC order applicable to providers of services in financial assets relating to cryptocurrencies imposes certain requirements, such as keeping a record of the IP address and public keys used by customers. Regulated service providers must: check and verify the identity of their customers; obtain identification documents; perform a KYC process; report large or out-of-the-ordinary transactions; and maintain records and documents. There is, however, a partial exemption for "casual customers", provided that the volume of their transaction does not exceed NIS 50,000 per six months.

Promotion and testing

Between 2018 and 2019, the ISA issued circulars about virtual currency, expressing its intention to establish a regulatory sandbox dedicated to blockchain-based projects. The proposed sandbox was designed to permit the issuance and trading of tokens, potentially categorised as security tokens, subject to specific reporting requirements and risk-mitigation measures, which were intended to be assessed on a case-by-case basis. Unfortunately, the implementation of the proposed sandbox, aimed at unifying all relevant regulatory entities, has yet to be carried out.[26]

In June 2020, the Israeli government introduced a preliminary bill to facilitate fintech development, outlining provisions for start-up companies in the fintech sector, including those engaged in blockchain projects, to operate within a regulatory sandbox under the supervision of the most applicable regulatory authority. This primary regulatory body would also serve as the central point of contact for these start-ups and would obtain approval from other relevant regulatory authorities. Notably, the legislative process for this draft bill has yet to commence.

In 2022, the ISA, in collaboration with the Innovation Authority, launched its fifth Data Sandbox Program for fintech companies specialising in payment and account information services. The programme was designed to promote innovation that increases efficiency and competition in Israel's capital markets and financial sector. For the first time, the Bank of Israel also participated as an observer, evaluating fintech applications based on their innovation, potential contribution to the economy, and regulatory feasibility. The programme aligns with the ISA and the Bank of Israel's efforts to enhance technologically advanced financial services for the public and foster competition in the market by expanding fintech activities in Israel. The focus of the Data Sandbox Program was addressing key challenges in Israel's financial system, particularly related to expanding public access to account information and innovative services through open APIs and integrating technological solutions in payments and interfaces between banks and fintech. In previous successful Data Sandbox Programs, 10 fintech companies were chosen out of 30 applicants.[27]

Ownership and licensing requirements

Investment advisors and fund managers

In Israel, individuals holding cryptocurrency as investment advisors or fund managers are subject to specific licensing requirements.[28] These requirements aim to safeguard investors' interests and ensure that those engaging in cryptocurrency investments possess the necessary expertise and experience. The primary obligation entails obtaining a licence from the ISA. Acquiring the licence entails passing a series of exams and meeting certain experience requirements. The ISA will consider several factors when making its decision, including the investment manager's experience, the riskiness of the investment, and the potential for money laundering.

Additionally, investment advisors and fund managers must fully comply with all applicable AML regulations. This includes maintaining comprehensive records of all cryptocurrency transactions and reporting any suspicious activities to the ISA. It is important to note that the licensing requirements for investment advisors and fund managers who hold cryptocurrencies are relatively new and are still being developed. It is possible that the ISA will impose further requirements in the future.

Custodians and institutional investors

In Israel, there is no legal requirement for digital assets to be transferred to or kept with a custodian; hence, the use of custodians is voluntary. However, institutional investors

are required to retain assets under custodian care, regardless of whether these assets are categorised as securities or cryptocurrencies. In September 2022, the Capital Market Authority published a circular draft addressing the safeguarding of financial assets, including legal tender (fiat) and virtual currencies. The draft determined that service providers must possess the skill and technological means required for safeguarding virtual currencies.

The provision of services that include the safekeeping of cryptoassets requires a licence pursuant to the Financial Services Law. Furthermore, custodians are subject to AML/CTF duties, including the identification of their non-casual customers, monitoring of transactions, reporting and recordkeeping.

Broker-dealers

In 2020, the Israeli government released a preliminary draft of the Broker-Dealer Law, which is intended to govern the activities of brokers and dealers. However, the official legislative process for enacting the law has not yet commenced.

At the time of writing, the activities of broker-dealers in Israel are only partially regulated, and in so, include the following:

(1) activities that involve providing investment advice, marketing investments or providing discretionary portfolio management are subject to licensing requirements pursuant to the Regulation of Investment Advice, Investment Marketing, and Investment Portfolio Management Law of 1995; and
(2) offering non-sophisticated investors securities that are traded on foreign exchanges is not allowed, aside from certain exceptions.

Mining

Cryptocurrency mining is neither prohibited nor permitted in Israel. Currently, there is no regulation surrounding this activity, apart from duties relating to tax reporting and payments. It is important to note that crypto mining is considered a business activity and is therefore subject to corporate income tax.

Border restrictions and declaration

In matters pertaining to cryptocurrency regulation, Israeli regulators recognise that certain activities may not inherently be regarded as activities conducted within the territorial boundaries of Israel, thereby impacting the applicability of the Israeli regulatory framework.

In practice, there are no current border restrictions or obligations to declare cryptocurrency holdings. However, there is legal uncertainty surrounding the "import" of cryptoassets. Sections 16 and 26(b) of the Israeli VAT Law of 1975 states that when importing an intangible asset, VAT applies to the owner of the goods. Nonetheless, there appears to be a lack of enforcement of the aforementioned sections. As a result, the enforcement of VAT obligations for the importation of intangible assets remains relatively uncharted.

Reporting requirements

At present, Israeli law exclusively imposes restrictions on cash transactions, thereby leaving virtual currency unaffected by legal limitations. The distinction lies in the classification of virtual currency, which is not deemed equivalent to conventional "cash" under the prevailing legal framework. Consequently, virtual currency transactions remain unregulated by any specific legal prohibitions.

Estate planning and testamentary succession

In matters concerning estate planning and testamentary succession, the treatment of cryptocurrencies is currently void of specific regulatory guidelines. Consequently, the principles for handling such assets are governed by the prevailing general civil laws, which are primarily determined by the provisions of the Succession Law. As a result, the disposition and distribution of cryptocurrencies within the context of inheritance and estate matters are subject to the application of these broader civil legal principles.

* * *

Endnotes

1. Income Tax Circular 5/2018 on the subject of taxation activity by means of decentralised payment (known as "virtual currencies").
2. https://www.nevo.co.il/law_html/law01/501_439.htm
3. https://www.boi.org.il/en/economic-roles/payment-systems/future-payment-methods/digital-shekel-cbdc
4. https://www.isa.gov.il/sites/ISAEng/1489/1511/Pages/eitinot220318.aspx
5. https://www.isa.gov.il/sites/ISAEng/1489/1513/Documents/FinalCryptoReportENG.pdf
6. *SEC v. W.J. Howey Co.*, 328 U.S. 293, 301 (1946).
7. Government Decision No. 204 of February 24, 2023 promotes the regulation of digital asset activities.
8. https://www.gov.il/he/Departments/publications/Call_for_bids/kol-kore-dao
9. https://www.isa.gov.il/Download/IsaFile_6025.pdf
10. Proposal Published for Public Commentary on Legislative Amendments Concerning the Applicability of Securities Laws for Digital Assets.
11. https://www.isa.gov.il/Download/IsaFile_6025.pdf
12. See Article 88 of the Income Tax Ordinance.
13. Circular 5/2018, *supra* note 1.
14. Circular 7/2018 – income tax on the subject of ICO – issuance of "digital tokens" for the provision of services and/or products under development (utility tokens).
15. Circular 91/2021 – income tax on the subject of conversion of decentralised means of payment called "virtual currencies".
16. https://www.gov.il/he/departments/news/superviser_bank_23112021
17. https://www.gov.il/en/departments/news/press_28112022
18. Bill to Amend the Income Tax Ordinance (Taxation of the Sale of Digital Coins), 2020.
19. See Article 11(a)(7) of the Financial Services Law.
20. https://www.isa.gov.il/sites/ISAEng/Pages/unregulated-investments.aspx
21. Circular 5/2018, *supra* note 1.
22. Circular 91/2021, *supra* note 15.
23. See *supra* note 18.
24. See Article 11(a)(7) of the Financial Services Law.
25. See Articles 14 and 16 of the Money Laundering Order.
26. https://innovationisrael.org.il/en/search/content?keys=innovation
27. https://www.isa.gov.il/sites/ISAEng/1489/1511/Pages/hodea1622.aspx
28. https://www.isa.gov.il/sites/ISAEng/2812/Pages/2814.aspx

Uri Zichor
Tel: +972 3 694 4162 / Email: uzichor@fbclawyers.com

Adv. Uri Zichor is a Hi-Tech, Technology & Venture Capital partner and heads FISCHER's Blockchain practice. Adv. Zichor has over a decade of experience in fintech, blockchain and cryptocurrencies. In the last decade, Adv. Zichor has represented a wide range of hi-tech companies, from start-ups in their initial growth stages, to emerging companies and unicorns, to public companies in Israel, the United States and Canada operating in a variety of fields, especially fintech and blockchain.

Prior to joining FISCHER, Adv. Zichor was one of the founders and leaders of the Fintech and Blockchain department (2016) of accounting firm EY Israel and was a member of the firm's global blockchain team. In his professional activities, he has managed and led complex transactions in diverse content worlds in the field of blockchain in connection with tax issues, regulation, auditing, operations and more.

Adv. Zichor advises companies from "establishment to sale/issuance" – he has rich experience in advising issuances, mergers, and acquisitions, both on the part of the purchaser and the purchased, and significant financing rounds, in providing ongoing counsel for companies in the process of formation and in the early stages of operation, and counselling them in areas of taxation, advisory, finance and auditing.

FISCHER (FBC & Co.)

146 Menachem Begin Rd., Tel Aviv 6492103, Israel
Tel: +972 3 694 4111 / URL: www.fbclawyers.com

Italy

Massimo Donna & Chiara Bianchi
Paradigma – Law & Strategy

Government attitude and definition

The demise of FTX in November 2022 was a hard blow for the crypto world. In fact, it not only triggered a market crash involving pretty much all crypto assets, but seriously dented the reputation of even the major crypto exchanges. As a result, traditional financial firms backtracked on most partnership plans with crypto players, and financial regulators' and supervisors' warnings on the risks of crypto assets became louder. The repercussions of such an environment reverberated on the non-financial business environment as well, with crypto firms passed from being the most sought-after sponsors to being snubbed by most sports teams (it did not help that two of the major football teams had been reportedly involved in court disputes with their crypto sponsors). Such a situation was soon dubbed "Crypto Winter", and worsened in the following months as a result of the US Securities and Exchange Commission cracking down on a number of crypto firms, including by way of filing lawsuits against some of the largest crypto exchanges for allegedly breaching financial regulations. The regulatory crackdown in the US reinvigorated Italian regulators, who voiced their concerns about the risks posed by crypto assets. In particular, Mr Fabio Panetta, a member of the European Central Bank's ("**ECB**") Executive Committee and soon to be appointed Governor of the Bank of Italy, posted a heated article criticising the crypto industry and warning about the risks of contamination of traditional finance (https://www.ecb.europa.eu/press/key/date/2022/html/ecb.sp221207_1~7dcbb0e1d0.it.html). It should be noted that such warnings followed in the footsteps of similar initiatives by regulators and supervisors preceding the Crypto Winter. For example, in June 2022, the Bank of Italy published a "*Communication of the Bank of Italy as regards decentralised technologies in finance and crypto-activities*" in which, after summing up the then current state of the proposed cryptocurrency regulations at the EU level – especially the proposed Markets in Crypto-Assets Regulation ("**MiCA**") – it urged banks, financial intermediaries and other operators to adopt utmost caution when dealing with crypto assets. Noticeably, in the communication, the Bank of Italy – borrowing certain definitions from MiCA – warned against using unbacked crypto assets either for payment or investment purposes.

However, whilst regulators heightened their warnings on the risk of crypto assets and crypto trading in the wake of the FTX catastrophe, they were never dismissive of the use cases and potential of blockchain technology and distributed ledger technology ("**DLT**") upon which crypto assets are designed. In fact, boosting the adoption of digital technologies has been a priority for Italy's government over the past few years. To this end, dedicated government schemes have been set up to fund digital start-ups as well as to promote and finance Artificial Intelligence as a means to innovate business practices. Such initiatives are especially aimed at industries that, traditionally, have been the cornerstone of the Italian business community,

such as fashion, food, art and hospitality, but also specialist industrial sectors. In this context, blockchain has been the centrepiece of the government's efforts to promote innovation, and the Crypto Winter was not going to reverse the government's or national regulators' attitude on non-crypto blockchain use cases. In fact, it should be noted that, even before the FTX debacle, the efforts to promote blockchain-based technologies were not without contradictions, with law-making efforts often followed by slow rule implementation on an administrative policy level and contradictory signals coming from regulators.

Furthermore, Italy has also passed legislation aimed at introducing a statutory definition of blockchain and smart contracts. In fact, by way of Law Decree no. 135/2018, DLTs have been defined as follows: "*Technologies and IT protocols which make use of a ledger which is shared, distributed, replicable, simultaneously accessible, with a decentralized architecture based on cryptography such that it allows for the recording, validation, updating, storing of verifiable data by each participant, non-alterable and non-modifiable.*" Such an attempt to provide a statutory definition of DLTs has been received critically by a number of commentators, but the government has informally signalled that it would be happy to amend it if need be. In particular, critics have pointed out that the definition of DLT does not seem to include permissioned blockchain in which, depending on the applicable governance rules, administrators may be allowed to alter ledgers, in determined circumstances.

Law Decree no. 135 of 2018 also provides a definition of smart contracts as a software programme that operates on DLTs and whose execution automatically binds two or more parties based on pre-determined arrangements between the same parties. However, whilst there seems to be consensus among legal commentators as to what smart contracts cannot do (i.e. they cannot disapply Italian imperative contract laws), very different interpretations have been construed as to their nature. To date, the most agreeable theory considers smart contracts as a contractually agreed method to ensure contract enforcement. In June 2023, the Bank of Italy launched a public consultation on the use of smart contracts in the banking and financial sector. It is hoped that the outcome of such consultation will bring clarity not only in terms of use cases, but also in respect of regulatory definitions.

The definitory landscape was then broadened by way of introduction of Law Decree no. 25 of 17 March 2023, soon fully converted into law by way of Law no. 52 of 10 May 2023, which was required to allow the full application of EU Regulation no. 2022/858, the EU DLT Pilot Regime ("**Fintech Decree**"). In fact, article 1 of the Fintech Decree includes a definition of DLT by way of reference to article 2 of the EU DLT Pilot Regime. Aside from its definitory merits, the Fintech Decree has not only allowed the full application of the EU DLT Pilot Regime in Italy, but has gone beyond the boundaries of European legislation by introducing the possibility of tokenising Financial Instruments that are not traded on MiFID II-regulated trading venues. Such non-tradable Financial Instruments can only be tokenised under the supervision of a ledger supervisor (*Responsabile del Registro*), typically a bank, a financial intermediary or an entity belonging to *ad hoc* categories as per the Fintech Decree. In July 2023, CONSOB (*Commissione Nazionale per la Società e la Borsa*), the Italian financial markets regulator and supervisor, launched a public consultation on its soon-to-be-adopted regulation on tokenised Financial Instruments. Although the Italian legal system does not include a general definition of cryptocurrencies, a statutory definition of "virtual currencies" for anti-money laundering ("**AML**") purposes has been included in Legislative Decree no. 90 of 2017, which was amended to transpose in Italy the EU Anti-Money Laundering Directives, as follows: "*[A] digital representation of value, which has not been issued or backed by a central bank or a public authority and which is not necessarily pegged to a legal tender, but which is used as a means of exchange for the purchase of goods or services or*

for investment purposes, and may be transferred, stored or negotiated electronically." The Italian legal system does not include a general definition of cryptocurrencies or crypto assets, and is not expected to introduce one before the coming into effect of MiCA. Therefore, commentators have debated whether cryptocurrencies should be regarded as currency or goods from a legal standpoint. This is not just a theoretical issue, as it would have an immediate effect on a number of levels, including whether or not cryptocurrencies are suitable means of payment. After years of debate and uncertainty, consensus seems now to have been reached in the sense that cryptocurrencies are subject to the same legal regime as currencies that are not legal tender in Italy, e.g. outdated currencies, such as the Italian Lira, which has been replaced by the Euro, and currencies of another country. Based on this theory, if a contractual payment is stipulated in a cryptocurrency, whilst the creditor is not entitled to payment in a currency other than that which was contractually agreed, the debtor can also make the payment in the currency having legal tender at the exchange rate of the date on which the payment obligation becomes due. Although, to date, no case law has confirmed such theory, it has been applied in an arbitration ruling (https://giustiziacivile.com/system/files/allegati/arbitro_unico_marcianise_-_14_aprile_2018_lodo_arbitrale.pdf).

As for the legal nature of cryptocurrencies, it should be pointed out that Italian Courts have not always aligned with the majority of commentators. In fact, the Italian Supreme Court has recently regarded the online sale of Bitcoin as the promotion of Financial Instruments, whilst the Court of Florence has labelled certain cryptocurrencies, which were held in deposit at an e-wallet and exchange outfit that later became insolvent, as "fungible goods" (Court of Florence, ruling no. 18 of 2019).

Also noteworthy is a ruling of the Court of Brescia of 2018 (Decree no. 7556 of 18 July 2018) in which the Court clarified the requirements that crypto assets must meet to be eligible to be paid in as share capital of a *Società a Responsabilità Limitata* (broadly speaking, the Italian equivalent of a limited liability company). In fact, the Court confirmed that cryptocurrencies are eligible to be paid in as share capital on the condition that their value is determinable, typically as determined in broadly used exchanges. Hence, the request of certain shareholders to increase the company's share capital by paying in certain currencies that they had just created and negotiated on a very small, homemade crypto exchange has been quashed by the Court. As for determining the legal nature of cryptocurrencies, the ruling of the Court of Brescia has not shed additional light, as it merely mentioned that under Italian law, both goods and services, in addition to cash, may be paid in as share capital.

Although, in the political arena, there have been talks of adopting "parallel cryptocurrencies", nothing has ever come of it for fear that their implementation would impact the monetary policy that, as Italy is a Euro area country, is the exclusive responsibility of the ECB.

Crypto asset regulation

When deciding how to regulate crypto assets, the Italian financial markets and banking regulators had to contend with Italians' irresistible draw to everything crypto, with some statistics placing the percentage of Italian families that have invested in crypto assets at a staggering 35%. Eventually, unlike other EU countries, Italy chose not to adopt any domestic crypto asset regulation, limiting itself to requiring firms operating crypto exchanges, crypto wallets or offering other services in connection with crypto assets to enrol with an *ad hoc* section of the Register of Financial Agents and Credit Mediators ("**OAM Register**") for AML purposes. Of course, should crypto exchanges offer additional products or services that fall within the definition of investment services or activities, they should be subject to

MiFID II – principally transposed in Italy by way of amending the Capital Markets Code (*Testo Unico della Finanza* or "**TUF**"). Italy has chosen to await the coming into effect of MiCA without adopting a domestic crypto assets regime in the interim.

Navigating a regulatory grey area

Thus, the use, storage and exchange of virtual currencies is not prohibited, although, over the years, both the Bank of Italy and CONSOB have issued quite stern warnings on the perils of cryptocurrencies. In fact, the banking regulator and the financial watchdog have pointed out the risks, respectively, for the banking system and for Italian investors of relying on still-unregulated technology and investment assets. Such warnings, however, do not appear to question the significance of crypto assets or imply that they will not increasingly play an important role going forward, but only remind the public of the current risks associated with them in the current unregulated landscape.

Also, from a data protection standpoint, crypto exchanges and crypto wallet service providers must be regarded as data controllers with respect to their customers' private keys as well as any other personal data that they process. In fact, one of the most significant obligations that they must carry out as per article 32 of the EU General Data Protection Regulation is to adopt and maintain security measures adequate to the outcome of an *ad hoc* Data Protection Impact Assessment. The punctual performance of such an obligation on the part of the firms operating crypto exchanges and crypto wallets is of particular significance since the appropriation of the customers' private keys by malicious third parties may result in the loss of the cryptocurrencies, with some crypto assets that, given their characteristics, may be nearly impossible to trace.

Of course, if crypto exchanges and crypto wallet service providers must adopt adequate security measures on the one hand, then any third parties who carry out hacks to steal the holders' private keys and take control of the cryptocurrencies may be criminally sanctioned on the other hand. In fact, under section 640-*ter* of the Criminal Code, those who alter an IT or network system or unlawfully tamper with data contained therein for a profit, causing damage to third parties, may be punished with imprisonment of up to three years as well as a fine of up to EUR 1,032. Imprisonment of up to six years and financial sanctions up to EUR 3,000 may be applied if the crime was perpetrated by way of stealing or unlawfully using a third party's digital identity, which may, in fact, consist of the victim's private keys. Phishing is regarded, and punished, as hacking.

Cryptocurrencies as an investment/sales regulation

MiFID II-regulated Financial Instruments and Financial Products

CONSOB has long been concerned with protecting retail investors to whom cryptocurrencies or crypto assets are offered, typically through the Internet. In fact, crypto assets are still considered a risky asset class, because of both their extreme volatility and opacity. Whilst most crypto assets do not fall within the definition of Financial Instruments as set out in MiFID II and transposed in the Italian legislation, they may be regarded as Financial Products, which are defined in the TUF as any type of financial investments different from Financial Instruments. Over the years, CONSOB has clarified this notion, stating that a three-pronged test must be passed for a financial investment to be regarded as a Financial Product: (1) funds must be deployed; (2) there is a promise or at least an expectation of a financial return; and (3) the relevant investor takes up a risk that is directly connected to the funds' deployment. Should a cryptocurrency pass such test, it would be regarded as a Financial Product and be subject to the national financial regulations as set out in the TUF.

In particular: (a) pursuant to article 94-*bis* of the TUF, a draft prospectus will need to be filed with CONSOB and obtain its approval before its final version is published and the relevant Financial Products are offered to Italian customers, for example, through Initial Coin Offerings ("**ICOs**"); and (b) the requirements for distance offers must be met. Of course, such obligations are only triggered if the Financial Products are offered to potential Italian customers. In this respect, typically CONSOB regards crypto assets as targeting Italian customers when they are offered through a website in Italian; however, in some recent decisions, the financial watchdog appeared to have taken a harder stance, claiming that an offer was directed at Italian customers simply because the website owner had not taken any active measures to prevent Italian customers from accepting the offer.

In this context, the Italian Supreme Court (ruling no. 26807 of 25 September 2020) has added additional uncertainty, as it has sentenced certain individuals to harsh criminal punishment for selling Bitcoins on the web for investment purposes. In fact, the Supreme Court found that, given the methods and context within which the Bitcoins were promoted, they should have been regarded and authorised as Financial Instruments.

NFTs

Equally uncertain is the legal regime of Non-Fungible Tokens ("**NFTs**"). Defining NFTs is no easy exercise, as the sheer mention of securities may raise issues on a number of levels, especially on the financial markets front. NFTs can be defined as digital instruments incorporating rights that can be exchanged on blockchain-based platforms. In some use cases, NFTs appear to undoubtedly pass the above-mentioned Financial Product tests, as they (1) are offered against the payment of funds, (2) with the express or implicit promise or expectation of a financial return, and (3) with the relevant investor accepting the risk of losing the deployed funds. For example, an NFT granting certain rights on certain specific artwork could be offered to the public for consideration, without it being considered a Financial Product. However, if the NFT issuer granted the NFT purchaser the right to sell the NFT back to the issuer after a certain time period for an agreed amount of fiat money or cryptocurrency that is higher than the paid price, then the NFT would typically be regarded as a Financial Product. Equally, if the NFT issuer marketed the NFT stressing the fact that it could be traded on the issuer's proprietary platform or on the secondary market at a likely or very likely premium, then the NFT would likely be held to be a Financial Product as well.

In this context, the nature of fractional NFTs ("**F-NFT**") has been widely scrutinised as the fractionalisation may be regarded as a way to turn NFTs into fungible tokens. In fact, once an artwork is fractioned into several F-NFTs, which are indistinguishable – and therefore fungible – among themselves, the distinction between NFTs and F-NFTs tends to fade away. Some critics have probably taken such reflections too far, arguing that F-NFTs should be regarded, *per se*, as Financial Products as F-NFT holders would only be interested in yielding a financial return on the tokens. In fact, financial gain is only one of the possible reasons for purchasing F-NFTs. For example, F-NFTs representing rights on certain specific artwork may be purchased for the sheer pleasure of being the stakeholder in such artwork, to support an artist or a cause, etc.

NFTs may find their principal use case in the Metaverse. Although the Metaverse is still an undefined, somehow nebulous notion (e.g. is the Metaverse going to be just the next generation of digital gaming or a whole life digital-twin? Will the Metaverse be one open platform, or will there be a number of proprietary Metaverses – possibly owned by Big Tech companies – competing to attract members/users?), the consensus appears to be that NFTs will play a major role in the Metaverse(s). However, if NFTs in the Metaverse ("**M-NFTs**")

can be purchased by the issuer and perhaps exchanged in the secondary market, then the treble Financial Product test will need to be carried out to determine the applicable legal regime. It appears evident that M-NFTs, which are granted interoperability across gaming platforms within the Metaverse, or across Metaverses (on the assumption that a number of them will coexist), will be more liquid, more easily tradeable on exchanges and, therefore, more likely to be regarded as Financial Products.

Contracts for difference ("**CFD**")

A CFD is an agreement between a "buyer" and a "seller" to exchange the difference between the current price of an underlying asset (shares, currencies, commodities, indices, etc.) and its price when the contract is closed. Also, if a CFD underlying asset is a crypto asset, the relevant CFD could be regarded as a Financial Instrument, with the consequence that the entity managing the platform/venue where the CFD is exchanged will need to comply with the investment services and activities (MiFID II) regime.

Money transmission laws and AML requirements

EU Directive no. 2018/843 ("**AML 5 Directive**") was implemented in Italy by way of Legislative Decree no. 125 of 2019 ("**Decree 125**"). In fact, even before transposing such directive into its legal system, Italy had imposed strict KYC and AML requirements upon crypto exchanges, but with the implementation of the AML 5 Directive, AML obligations have also been imposed upon crypto wallet service providers. In addition, both crypto exchange and crypto wallet providers must now enrol with the OAM Register. Decree 125 has also clarified the definition of crypto exchange, which, under the previous regime, was limited to firms exchanging fiat money with cryptocurrencies and the other way around, whilst the new rules also apply to the activity of converting a certain cryptocurrency into another cryptocurrency. AML provisions also apply to any "*provider of services relevant to the use of virtual currencies*" that provides services instrumental to the issuing, offering, transfer and settlement as well as any other services aimed at the acquisition, negotiation, and intermediation of cryptocurrency exchanges (along with exchange and wallet service providers, the "**Crypto Service Providers**"). The lawmaker's intent was, of course, to cast its net as wide as possible to encompass as many crypto activities as possible within the field of application of Decree 125.

As for the specific AML obligations imposed upon Crypto Service Providers, they include adequate customer due diligence, record retention and suspicious transaction reporting.

In fact, Crypto Service Providers must provide adequate information as to the provenance of the funds that their customers request them to store, exchange or settle against other positions as well as on the identity of their customers, including, for example, their profession and tax status, residence, or residence in terrorism-financing countries, etc. Customer due diligence, however, must not only be carried out when "onboarding" a customer, but must also continue over time by way of monitoring the relevant customer's operations (e.g. has the customer tried to fly below the radar by fragmenting fund transfers? Has the customer focused his/her activities on Altcoins that impede tracing?, etc.).

For a period of 10 years, Crypto Service Providers must also retain records of documents, data, and information instrumental to preventing, identifying or ascertaining potential money-laundering or terrorism-funding activities that may be useful in order for the relevant financial investigation authorities to do their job.

Finally, Crypto Service Providers must report suspicious transactions to the competent authorities.

From 16 May 2022, all crypto exchange and crypto wallet providers operating in Italy are required to enrol with the OAM Register. Applicants can be either individuals or legal persons, in the latter case incorporated in Italy or – if incorporated in another EU Member State – having set up a permanent establishment in Italy. The OAM may accept or reject applications within 15 days of their filing, and applicants cannot start operating until their application has been accepted (*ad hoc* interim provisions were set forth for exchanges and wallets already transacting business in Italy before the OAM Register was set up). The initial OAM membership fee is EUR 500 if the crypto exchange or wallet is operated by an individual and EUR 8,300 if it is operated by a legal person; however, the OAM has recently introduced additional fees as follows: an annual fixed fee of EUR 200 for individuals; an annual fixed fee of EUR 1,500 for legal persons; and a variable fee based on the number of transactions carried out by the relevant member (EUR 0.10 for each record).

Promotion and testing

Another sign that the general approach to financial technology was shifting was the inclusion of specific measures aimed at setting up a Sandbox Programme for projects in the banking, finance and insurance sector in Law Decree no. 34 of 2019, a piece of legislation dubbed the "Growth Decree" as it was meant to boost the Italian economy. The Growth Decree was subsequently transposed into full law by way of Law no. 58 of 28 June 2019, and on 30 April 2021 the Ministry of Economy and Finance adopted Decree no. 100, setting up in detail the requirements and workings of the first Italian Fintech Sandbox Programme ("**FSP**"). Since its inception, the FSP has accepted fintechs operating (or wishing to operate) in a broad range of fields, from DLT-based investment funds to the placement of Financial Instruments through DLT solutions, instant lending, algorithmic credit scoring, etc. It is also worth noting that some of the projects admitted to the FSP belong to, or are sponsored by, smaller banks, which proves that even smaller actors are embracing DLT and, in general, financial innovation.

Mining

In a recent ranking by cost of mining, Italy was ranked the most expensive country for Bitcoin mining due to the high energy cost. Mining is not subject to any specific regulation.

Massimo Donna
Tel: +39 02 3655 2788 / Email: md@paradigma-law.com
Massimo is head of the Technology Group at Paradigma – Law & Strategy. He advises clients on a broad range of technology and complex commercial matters. Massimo also advises clients on employment tech matters. Massimo was educated in Italy and Spain, trained in Italy and New York City and practised law as a foreign lawyer in London. Massimo also served as a senior in-house lawyer at various multinational tech companies. His mother tongues are Italian and English and he is also fluent in Spanish and French. Massimo routinely lectures on a range of technology law matters.

Chiara Bianchi
Tel: +39 02 3655 2788 / Email: cbianchi@paradigma-law.com
Chiara is a Partner at Paradigma – Law & Strategy. She advises clients on technology and commercial matters, including cybersecurity and technology-driven M&A. Chiara is an experienced litigator and also advises clients on compliance-related issues.

Paradigma – Law & Strategy

Piazza Luigi Vittorio Bertarelli 1, 20122 Milan, Italy
Tel: +39 02 3655 2788 / URL: www.paradigma-law.com

Japan

Takeshi Nagase, Takato Fukui & Keisuke Hatano
Anderson Mōri & Tomotsune

Regulatory framework and definition

General overview

In Japan, there is no omnibus regulation governing blockchain-based tokens. The legal status of tokens under Japanese law is determined based on their functions and uses.

For example, cryptocurrencies and utility tokens such as BTC, ETH, etc. are regulated as "Crypto Assets" under the Payment Services Act (the "**PSA**"). Business operators who engage in the business of buying, selling or exchanging Crypto Assets (as well as in the intermediation of such activities), or in the management of Crypto Assets for the benefit of others, are required to undergo registration as a provider of Crypto Asset Exchange Services ("**CAES**" and a provider of CAES, a "**CAESP**"). Currency denominated stablecoins such as USDC and USDT are regulated as "Electronic Payment Instruments" ("**EPIs**") under the PSA. Business operators who engage in the business of buying, selling or exchanging EPIs (as well as in the intermediation of such activities), or in the management of EPIs for the benefit of others, are required to undergo registration as an Electronic Payment Instruments Exchange Service Provider ("**EPIESP**"). However, so-called algorithmic stablecoins that are not collateralised by fiat currency but whose values are linked to fiat currency through algorithms do not fall within the category of EPIs as they do not qualify as Currency Denominated Assets. Instead, such algorithmic stablecoins will constitute Crypto Assets if they are transferable or tradeable *vis-à-vis* unspecified parties on a blockchain.

So-called "security tokens", which represent shares, bonds or fund interests in tokens, are regulated under the Financial Instruments and Exchange Act (the "**FIEA**") as electronically recorded transferable rights ("**ERTRs**") to be indicated on securities, etc. ("**ERTRIS, etc.**"). A business operator who engages in the business of offering (including the handling of such offers), buying, selling or exchanging ERTRIS, etc. (as well as in the intermediation of such activities) is required to undergo registration as Type I Financial Instruments Business Operators ("**Type I FIBOs**").

Tokens other than those mentioned above, such as non-fungible tokens ("**NFTs**"), which have no economic function as a means of payment due to their unique characteristics, will not be regulated in principle under the current regulatory framework.

Introduction of regulatory framework for stablecoins

On March 4, 2022, the "Bill for Partial Amendment to the Act on Payment Services Act, etc. for the Purpose of Establishing a Stable and Efficient Funds Settlement System" (the "**Amendment Act**"), which aims to introduce new regulations in respect of stablecoins, was submitted to the Diet. The Amendment Act was approved on June 3, 2022 and came into effect on June 1, 2023.

Under the Amendment Act:

(i) EPIs (i.e., currency denominated stablecoins) are distinguished from other currency denominated assets by the following factors: (i) whether they can be used as payment for consideration to unspecified persons; and (ii) whether they may be purchased from or sold to unspecified persons. Based on this, prepaid payment instruments and electronic currency that are issued by fund transfer service providers do not satisfy condition (i), as their issuers would centrally manage the balance of each user and the scope of stores (that is, member stores) that accept the relevant prepaid payment instruments and electronic money. Additionally, digital currencies, notwithstanding that they are issued on blockchains, will not satisfy condition (ii) if their issuers have taken technical measures that restrict the transfer of such digital currencies only to persons who have been verified as unproblematic under know-your-customer ("**KYC**") checks at the time of transaction, and if the issuers' consent or other involvement is required for every transfer of the digital currencies. Consequently, stablecoins issued on a permissionless blockchain would typically be deemed EPIs, as new holders of such stablecoins generally are not required to undergo KYC checks and transfers of such stablecoins do not require the involvement of their issuers.

(ii) Those who are permitted to issue EPIs directly to Japanese residents are limited to banks, fund transfer service providers, trust banks or trust companies that are licensed in Japan. This is because the issuance and redemption of EPIs constitute "fund remittance transactions" (*kawase-torihiki*).

(iii) It is not possible for a CAESP to list EPIs on any exchange or manage EPIs for its users without being registered as an EPIESP.

(iv) An EPIESP is subject to anti-money laundering/counter-financing of terrorism ("**AML/CFT**") regulations, including a "travel" rule. More specifically, an EPIESP, when transferring EPIs to any other EPIESP, is required to provide a customer's identification information to such other EPIESP. Moreover, an EPIESP who sends or receives EPIs to or from overseas virtual asset service providers ("**VASPs**") on a regular basis is required to check whether such VASPs are conducting appropriate due diligence on its users for AML/CFT purposes.

Recent developments in respect of NFTs

Recently, digital art and digital trading cards represented by NFTs, which are non-replaceable digital tokens issued on a blockchain, have been traded for considerable amounts. As a result, NFTs have been rapidly gaining attention in Japan. While digital data is inherently free and easy to copy, NFTs are considered innovative because they involve creation of unique, one-of-a-kind data based on blockchain technology.

From the regulatory standpoint, NFTs would not constitute securities or ERTRIS, etc. under the FIEA if their holders do not share in profits or receive dividends. In addition, where NFTs are non-fungible, non-substitutable, and not used as a means of payment, they would not be deemed Crypto Assets under the PSA.

According to the FSA Administration Guidelines on Crypto Assets ("**Crypto Asset Guidelines**"), dated March 24, 2023 and issued by the Financial Services Agency of Japan (the "**FSA**"), one of the factors for determining whether a token constitutes a Type I Crypto Asset (defined below) is whether it is "an asset capable of being purchased or sold with legal fiat currency or crypto assets under socially accepted norms". Specifically, a token that satisfies items (i) and (ii) below generally will not constitute a Type I Crypto Asset. The same applies to the determination of whether a token constitutes a Type II Crypto Asset (defined below):

(i) The issuer has made it clear that the token is not intended to be used as payment for goods, etc. to unspecified parties. This can be achieved by, for example, stating clearly in the terms and conditions of the issuer or its business-handling service provider, or in the product description, that use of the token as a means of payment to unspecified parties is prohibited, or that the token or related system is designed in a way that does not enable it to be used as a means of payment to unspecified parties).

(ii) In situations where use of the token as a means of payment for goods, etc. to unspecified parties is permitted, certain requirements on the price and quantity of the relevant goods, etc., and on the technical characteristics and specifications of the token, must be met. For example, at least one of the following characteristics must be present:
   (a) the minimum value per transaction must be sufficiently high (i.e., JPY1,000 or more); or
   (b) the number of tokens issuable, in proportion to the aforementioned minimum value of a transaction, is limited (i.e., not exceeding 1 million).

Central bank attitudes toward cryptocurrencies

Under Japanese law, a Crypto Asset is neither treated as "money" nor equated with fiat currency. No Crypto Asset is supported by the Japanese government or the central bank of Japan (the Bank of Japan, or the "**BOJ**").

With that said, it should be noted that on July 2, 2020, the BOJ released a report entitled "Technological Challenges in Having Central Bank Digital Currencies Function as Cash Equivalents", summarising the technical issues involved in getting central bank digital currencies ("**CBDCs**") to function as cash equivalents. In the report, the BOJ also mentioned that it may, through feasibility studies, verify the possibility of using CBDCs as cash equivalents. In line with this, the BOJ conducted "Proof-of-Concept Phase 1" from April 2021 to March 2022 to establish an experimental environment using several design patterns for the CBDC ledger, which is the foundation of the CBDC system, and to verify whether the basic functions of CBDCs could be properly executed. In "Proof-of-Concept Phase 2", conducted from April 2022 to March 2023, following Phase 1, the BOJ added several peripheral functions to CBDCs, and particularly to functions related to the CBDC ledger verified in Phase 1, in order to ascertain certain important processing performance and technical capabilities in respect of the CBDC ledger. In Phase 2, the BOJ also looked at the possibility of applying new technologies to data models and databases in respect of CBDCs. The government of Japan has so far not decided whether to issue CBDCs in Japan, but discussions continue to be held in this regard. On its part, the BOJ believes it important to continue preparations for any future issuance of CBDCs, including the continued conduct of technical demonstration tests, so as to be able to respond in a timely manner to future changes in the external environment.

Cryptocurrency regulation

Under Japanese law, "Crypto Asset" is not listed as a type of "Security" as defined in the FIEA (please note, however, that a certain type of token may be subject to the regulation of the Act, as discussed later in the below section entitled "**Sales regulation**"). The PSA defines "Crypto Asset", and requires a person who provides CAES to be registered with the FSA. A person who conducts CAES without registration will be subject to criminal proceedings and punishment.

Therefore, the respective definitions of Crypto Asset and CAES are of crucial importance.

Definition of Crypto Asset

The term "Crypto Asset" is defined in the PSA as:

(i) proprietary value that may be used to pay an unspecified person the price of any goods, etc. purchased or borrowed or any services provided and that may be sold to or purchased from an unspecified person (limited to that recorded on electronic devices or other objects by electronic means and excluding Japanese and other foreign currencies and Currency Denominated Assets; the same applies in the following item) and that may be transferred using an electronic data processing system ("**Type I Crypto Asset**"); or

(ii) proprietary value that may be exchanged reciprocally for proprietary value specified in the preceding item with an unspecified person and that may be transferred using an electronic data processing system ("**Type II Crypto Asset**").

Though the definition is complicated, in short, a cryptocurrency that is usable as a payment method to an unspecified person and not denominated in a fiat currency falls under the definition of Crypto Asset.

"Currency Denominated Assets" means any assets that are denominated in Japanese or other foreign currency and do not fall under the definition of Crypto Asset. For example, prepaid e-money cards usually fall under Currency Denominated Assets. If a coin issued by a bank is guaranteed to have a certain value of a fiat currency, such a coin will likely be treated as a Currency Denominated Asset rather than a Crypto Asset.

Definition of Crypto Asset Exchange Services

Under the PSA, the term "Crypto Asset Exchange Services" (or CAES) means any of the following acts carried out as a business:

(a) sale or purchase of Crypto Assets, or the exchange of a Crypto Asset for another Crypto Asset;

(b) intermediating, brokering or acting as an agent in respect of the activities listed in item (a);

(c) management of customers' money in connection with the activities listed in items (a) and (b); or

(d) management of customers' Crypto Assets for the benefit of another person.

It should be noted that the PSA designates item (d) (management of customers' Crypto Assets for the benefit of another person) as a type of CAES. Consequently, management of Crypto Assets without the sale and purchase thereof ("**Crypto Asset Custody Services**") is included in the scope of CAES. Therefore, a person engaging in Crypto Asset Custody Services needs to undergo registration as a CAESP. In this context, the Crypto Asset Guidelines describes the "management of customers' Crypto Assets for the benefit of another person" as follows: "[A]lthough whether or not each service constitutes the management of Crypto Assets should be determined based on its actual circumstances, a service constitutes the management of Crypto Assets if a service provider is in a position in which it may transfer its users' Crypto Assets (for example, if such service provider owns a private key with which it may transfer users' Crypto Assets solely or jointly with its related parties, without the users' involvement)." Accordingly, it is understood that if a service provider merely provides its users with a Crypto Asset wallet application (i.e., a non-custodial wallet) and private keys are managed by the users themselves, such a service would not constitute a Crypto Asset Custody Service.

Principal regulations on CAESPs

Regulations for the handling of new Crypto Assets

Under the PSA, a CAESP who proposes to handle a new Crypto Asset is required to notify the FSA in advance. Additionally, the self-regulatory rules of the Japan Virtual and Crypto

Assets Exchange Association (the "**JVCEA**"), a self-regulatory organisation established under the PSA, require a member CAESP who wishes to deal in a new Crypto Asset to first conduct an internal assessment of such Crypto Asset and submit an assessment report to the JVCEA ("**JVCEA Pre-Assessment**"). As no new Crypto Asset can be handled if the JVCEA raises any objection, a member is effectively required to obtain the JVCEA's approval before it can begin to handle a new Crypto Asset.

In this regard, with effect from December 26, 2022, the JVCEA self-regulatory rules were amended to establish (i) a "Green List System" under which certain member CAESPs ("**Green List Eligible Members**") may be exempted from JVCEA Pre-Assessment in respect of certain Crypto Assets designated by the JVCEA, and (ii) the "Crypto Asset Self-Check System" ("**CASC System**") under which certain member CAESPs ("**CASC Eligible Members**") may generally be exempted from JVCEA Pre-Assessment except in certain specific circumstances. Under the Green List System, Crypto Assets that meet all of the following four criteria would be deemed "crypto assets widely handled in Japan" by the JVCEA (and designated as such on the JVCEA's webpage). No JVCEA Pre-Assessment is required for "crypto assets widely handled in Japan" if such Crypto Assets are handled by a Green List Eligible Member, for example:

(a) Crypto Assets that have been handled by three or more member CAESPs;
(b) Crypto Assets that have been handled by one member CAESP for at least six months;
(c) Crypto Assets for which the JVCEA has not set ancillary conditions for handling; and
(d) Crypto Assets that have not been deemed inappropriate for the Green List System by the JVCEA for any other reason.

It should be noted that, under the Green List System, only "crypto assets widely handled in Japan" may be exempted from JVCEA Pre-Assessment. What this means is that JVCEA Pre-Assessment is still required for other Crypto Assets in the same way as before (unless such Crypto Assets have undergone the CASC System).

Additionally, JVCEA Pre-Assessment is required only with respect to Crypto Assets being handled for the first time in Japan. Crypto assets handled by a Green List Eligible Member or a CAESP Eligible Member are not subject to JVCEA Pre-Assessment.

Protection of users' property

In Japan, due to a series of incidents involving leakage of Crypto Assets from CAESPs, strict regulations have been introduced for the protection of user property.

Under such regulations, a CAESP that manages users' fiat currency and Crypto Assets must segregate such property from its own property.

For purposes of fiat currency management, such currency must be held in trust with a trust bank or trust company for protection against the CAESP's bankruptcy.

In the area of Crypto Asset management, stringent rules, as set forth below, have been put in place to protect users from leakages of Crypto Assets and from the bankruptcy of a CAESP:

(a) A CAESP must manage users' Crypto Assets and its own Crypto Assets in separate wallets.
(b) A CAESP must manage at least 95% of users' Crypto Assets in wallets that are not connected to the Internet (so-called "cold wallets").
(c) A CAESP that manages less than 5% of its users' Crypto Assets in a wallet other than a cold wallet (so-called "hot wallets") must manage the same type and amount of its own Crypto Assets ("**Redemption Guarantee Crypto Assets**") in a cold wallet to protect users against the risk of leakages of Crypto Assets from hot wallets.

(d) Users will have preference rights to repayment over the segregated Crypto Assets and Redemption Guarantee Crypto Assets. Such priority security interest is specifically stipulated in the PSA.

In addition to the above, CAESPs are required to have their segregation of fiat currency and Crypto Assets audited annually by a certified public accountant or auditing firm.

Other regulations on the conduct of CAESPs

In addition, the following regulations are imposed on the conduct of CAESPs:

(a) CAESPs are required to take such measures as necessary to ensure the security of important information, such as personal information and information on private keys to Crypto Assets. They are also required to establish a risk management system to prevent system failures and cyber incidents. Establishment of contingency plans to deal with exigencies and provision of related training are also required.
(b) CAESPs are required to provide users with information such as an overview of each Crypto Asset handled by them, details of transaction rules and fees, information on the assets received from users, and users' transaction history.
(c) CAESPs are subject to regulations regarding CAES advertising and solicitation. False and misleading representations, as well as representations promoting the trading of Crypto Assets for the sole purpose of profit, are prohibited.
(d) CAESPs are required to establish internal control systems for responding to user complaints in a fair and appropriate manner, and to take measures to resolve disputes through alternative dispute resolution procedures.

Registration process for CAESPs

Applicants for CAESP status are required to be (i) stock companies (*kabushiki-kaisha*), or (ii) foreign CAESPs with an office(s) and representative in Japan and registered or licensed in the foreign country. Accordingly, any foreign entity wishing to register as a CAESP must establish either a subsidiary (in the form of *kabushiki-kaisha*) or a branch in Japan. However, there are no cases where registration in the form of a branch has been approved by the FSA. So far, all foreign CAESPs have established subsidiaries in Japan and have obtained registration of those subsidiaries.

In addition, applicants must have: (a) a sufficient financial base (i.e., a minimum capital of JPY10 million and positive minimum net assets); (b) a satisfactory organisational structure and certain internal systems for the appropriate and proper provision of CAES; and (c) internal systems to ensure compliance with applicable laws and regulations.

Applicants must submit a registration application containing, among others: (i) its trade name and address; (ii) the amount of its capital; (iii) the names of its director(s); (iv) the names of the Crypto Assets it will handle; (v) the contents of and the means by which it will provide the relevant CAES; (vi) the name(s) of outsourcee(s) (if any) and the address(es) thereof; and (vii) the method by which the management of its users' Crypto Assets will be segregated from the management of its own Crypto Assets.

A registration application has to be accompanied by certain documents, including: (i) a document pledging that there are no circumstances constituting grounds for refusal of registration; (ii) an extract of the certificate of residence of the applicant's directors, etc.; (iii) a résumé of the applicant's directors, etc.; (iv) a list of the applicant's shareholders; (v) the applicant's financial documents; (vi) documents containing particulars regarding the establishment of an internal system for ensuring proper and secure provision/performance of CAES by the applicant; (vii) an organisational chart in respect of the applicant; (viii) the applicant's internal rules; and (ix) a form of the contract to be entered into with users.

During the registration process, the FSA will request for applicants to complete a checklist consisting of more than 400 questions, in order to confirm that the applicants have established internal systems for the proper and secure provision of CAES. In addition, the FSA will separately prepare a detailed progress chart to confirm the checking process. The registration process essentially serves as a due diligence exercise by the FSA, by which the FSA will determine whether to approve an applicant's registration. "Registration", if granted, will be akin to the issuance of a "licence" to the applicant. In order to proceed with such a registration process, it is necessary to add a number of executives and employees with practical experience in Japanese financial institutions to the organisational chart, to develop dozens of internal regulations equivalent to those of financial institutions, to invest in systems to ensure that the services provided are appropriate, and to go through checks by the FSA.

Upon registration, the applicant's name will be added to the registry of CAESPs, which is made publicly available by the FSA.

Sales regulation

Overview

Cryptocurrencies (including Crypto Assets) do not fall within the definition of "Securities" under the FIEA, and the sale of Crypto Assets or tokens (including initial coin offerings, or "**ICOs**") is not specifically or directly regulated by the FIEA (although a certain type of token may be subject to the FIEA, as discussed below).

There are various types of tokens issued by way of ICO, and Japanese regulations applicable to ICOs vary according to the respective schemes.

Main types of tokens and applicable regulations

Crypto Asset type

If a token falls within the definition of Crypto Asset, it will be subject to Crypto Asset regulations under the PSA. In accordance with current practice, tokens that are (i) issued via ICO and already dealt with by Japanese or foreign exchanges would fall within the definition of Crypto Asset under the PSA, based on the rationale that exchange markets for such tokens must already be in existence, and (ii) not yet dealt with by Japanese or foreign exchanges, but are not restricted by their issuers from being exchanged with Japanese or foreign fiat currencies or Crypto Assets, would likely fall within the definition of Crypto Asset under the PSA.

According to the JVCEA's "Rules for Selling New Crypto Assets" (the "**ICO Rules**"), there are two types of ICO, which can be described as follows: (i) an offering where an Exchange Provider issues new tokens and sells such tokens by itself; or (ii) an offering where a token issuer delegates Exchange Providers to sell the newly issued tokens. Generally speaking, the ICO Rules stipulate the following requirements for each type of ICO:

(i) maintenance of a structure for review of a targeted business that raises funds via ICO;
(ii) information disclosure of the token, the token issuer's purpose for the funds, or the like;
(iii) segregated management of funds (both fiat and Crypto Assets) raised by ICO;
(iv) proper account processing and financial disclosure of funds raised by ICO;
(v) safety assurance of the newly issued token, its blockchain, smart contract, wallet tool, and the like; and
(vi) proper valuation of newly issued tokens.

Securities (equity interest in an investment fund) type

The concept of ERTRs is defined in the FIEA. This clarified the scope of tokens governed by the FIEA. Specifically, the concept of ERTRs relates to the rights set forth in Article 2,

Paragraph 2 of the FIEA that are represented by proprietary value that is transferable by means of an electronic data processing system (but limited only to proprietary values recorded in electronic devices or otherwise by electronic means), excluding those rights specified in the relevant Cabinet Office Ordinance in light of their negotiability and other factors. Although Article 2, Paragraph 2 of the FIEA refers to rights of various kinds, tokens issued in "security token offerings" ("**STOs**") are understood to constitute, in principle, "collective investment scheme interests" ("**CISIs**") under the FIEA. CISIs are deemed to have been formed when the following three requirements are met: (i) investors (i.e., rights holders) invest or contribute cash or other assets to a business; (ii) the cash or other assets contributed by investors are invested in the business; and (iii) investors have the right to receive dividends of profits or assets generated from investments in the business. Tokens issued under STOs would constitute ERTRs if the three requirements above are satisfied.

Simply put, rights treated as "Paragraph 2 Securities" (i.e., rights that are deemed securities pursuant to Article 2, Paragraph 2 of the FIEA) and represented by negotiable digital tokens will be treated as Paragraph 1 Securities unless they fall under an exemption. As a result of the application of disclosure requirements to ERTRs, issuers of ERTRs are in principle required, upon making a public offering or secondary distribution, to file a securities registration statement and issue a prospectus. Any person who causes other persons to acquire ERTRs or who sells ERTRs to other persons through a public offering or secondary distribution must deliver a prospectus to such other persons in advance or at the same time.

As ERTRs constitute Paragraph 1 Securities, registration as a Type I FIBO is required for the purposes of selling, purchasing or handling the public offering of ERTRs in the course of a business. In addition, any ERTR issuer who solicits acquisition of such ERTR (i.e., undertaking an STO) is required to undergo registration as a Type II FIBO, unless such issuer qualifies as a specially permitted business for qualified institutional investors.

Prepaid card type

If the tokens are similar in nature to prepaid cards and can be used as consideration for goods or services provided by token issuers, they may be regarded as prepaid payment instruments, which are subject to the relevant regulations of the PSA (in which case the regulations in respect of Crypto Assets in the same Act would not be applicable).

Introduction to regulations governing Crypto Asset Derivatives Transactions

The FIEA regulates Crypto Asset Derivatives Transactions by stipulating certain regulations in respect of Crypto Asset Derivatives Transactions, in order to protect users and ensure that such transactions are conducted appropriately. Specifically, for purposes of subjecting Derivatives Transactions involving "Financial Instruments" or "Financial Indicators" to certain entry regulations and rules of conduct issued under the FIEA, the FIEA includes "Crypto Assets" and "standardized instruments created by a Financial Instruments Exchange for the purposes of facilitating Market Transactions of Derivatives by standardizing interest rates, maturity periods and/or other conditions of (Crypto Assets)" in the definition of "Financial Instruments". Further, under the FIEA, prices, interest rates, etc. in respect of Crypto Assets constitute "Financial Indicators".

Since Crypto Assets are included in the definition of Financial Instruments, the conduct of Over-the-Counter ("**OTC**") Derivatives Transactions related to Crypto Assets or related intermediary (*baikai*) or brokerage (*toritsugi*) activities will also constitute Type I Financial Instruments Business. Accordingly, business operators engaging in these transactions need to undergo registration as FIBOs in the same way as business operators engaging in foreign exchange margin trading.

Any entity that intends to be a FIBO engaging in Type I Financial Instruments Business is required to meet certain asset requirements, including having:
(i) a stated capital of at least JPY50 million;
(ii) net assets of at least JPY50 million; and
(iii) a capital-to-risk ratio of at least 120%.

It should be noted that, traditionally, the registration requirements under the FIEA are not applicable to non-securities-related Derivatives Transaction services provided to certain professional customers. However, the registration requirements will be applicable to Crypto Asset Derivatives Transactions, regardless of the type of customers involved, in light of the high-risk nature of Crypto Asset Derivatives Transactions. However, foreign Crypto Asset Derivative Business Operators (i.e., companies that engage in Crypto Asset Derivatives Transactions in the course of a business in a foreign country, under applicable foreign laws and regulations) conducting OTC Crypto Asset Derivatives Transactions with certain professional entities in Japan will be excluded from the registration requirements in respect of the FIBOs. Such professional entities are:
(i) the government of Japan or the BOJ;
(ii) FIBOs and financial institutions that engage in OTC Crypto Asset Derivatives Transactions in the course of a business;
(iii) financial institutions, trust companies or foreign trust companies (provided they conduct OTC Crypto Asset Derivatives Transactions only for investment purposes or on the account of trustors under trust agreements); and
(iv) FIBOs who engage in investment management business (provided that such entities engage in activities related to investment management business).

Introduction to regulations governing unfair acts in Crypto Asset or Crypto Asset Derivatives Transactions

The FIEA contains the following prohibitions against unfair acts (the conduct of which is punishable by penalties) in respect of Crypto Asset spot transactions and Crypto Asset Derivatives Transactions, regardless of the violating party:
(a) prohibition of wrongful acts;
(b) prohibition of dissemination of rumours, usage of fraudulent means, assault or intimidation; and
(c) prohibition of market manipulation.

These prohibitions are intended to enhance protection of users and to prevent unjust enrichment.

However, insider trading is not regulated under the FIEA at this moment in time, due to difficulties in formulating a clear concept of Crypto Asset issuers, as well as the general inherent difficulties associated with the identification of undisclosed material facts.

Taxation

The National Tax Agency of Japan has announced that profits realised from the trading of Crypto Assets constitute "miscellaneous income" (*zatsu-shotoku*). The tax rate for miscellaneous income is progressive, ranging from 5% to 45% on profits. In addition to this, 10% of such profits are payable to the local government as inhabitant tax.

Taxpayers are able to utilise losses from Crypto Asset trading to offset such profits.

No consumption tax is imposable on the sale or exchange of Crypto Assets. However, consumption tax will be levied on lending fees and interest on Crypto Assets.

Furthermore, inheritance tax will be imposed upon the estate of a deceased person in respect of Crypto Assets that were held by such person.

Further, it was stated in the Japanese government's "Ruling Party's Tax Reform Proposal", published in December 2022, that year-end corporate taxation in respect of Crypto Assets would not apply to Crypto Assets held by a corporation at the end of a fiscal year if such Crypto Assets (i) are subject to valuation gains or losses based on market valuation, and (ii) meet certain requirements, such as if they have been issued by that corporation and have been continuously held since their issuance. As a result, on June 20, 2023, the National Tax Administration issued a "Partial Revision of the Basic Notification on Corporate Tax, etc. (Notification on Interpretation of Laws and Regulations)", which officially excludes from the scope of market valuation Crypto Assets held by a corporation at the end of its fiscal year that are issued by that corporation itself and meet the following conditions:

(a) The Crypto Assets were issued by that corporation and have been continuously held since their issuance.
(b) The Crypto Assets have been continuously restricted from being transferred by any of the following means since the date of their issuance:
    (i) certain technical measures have been taken to ensure that the Crypto Assets cannot be transferred to another party; or
    (ii) the Crypto Assets have been held in a trust that meets certain requirements.

Money transmission laws and anti-money laundering requirements

Money transmission

Under Japanese law, only licensed banks or fund transfer business operators are permitted to engage in the business of money remittance transactions. Money remittance transactions means, according to Supreme Court precedent, "to undertake the task of transferring funds requested by customers utilising the systems of fund transfer without transporting cash between distant parties, and/or to carry out such task". Technically speaking, Crypto Asset does not fall under the definition of "fund". However, if the remittance transaction of a Crypto Asset includes the exchange of fiat currencies in substance, such transaction will likely be deemed a money remittance transaction. Further, issuance of stablecoins, which are pegged to fiat currency, would be deemed engagement in money remittance transactions.

Anti-money laundering requirements

Under the Act on Prevention of Transfer of Criminal Proceeds, CAESPs are obligated to: (i) verify identification data of the customer and a person who has substantial control over the customer's business for the purpose of conducting the transaction and occupation of business; (ii) prepare verification records and transaction records; (iii) maintain the records for seven years; and (iv) report suspicious transactions to the relevant authority, and so forth.

Travel Rule

When a CAESP or an EPIESP transfers Crypto Assets or EPIs to a customer of another CAESP (including any foreign CAESP and EPIESP) at the request of a customer, the CAESP or EPIESP must notify the receiving CAESP or EPIESP of the identification information, including the name and blockchain address, pertaining to the sender and the receiver (the "**Travel Rule**"). However, transfers to a CAESP or an EPIEPS in countries that do not yet have any Travel Rule legislation are not subject to the rule. In addition, when a CAESP or an EPIESP transfers Crypto Assets or EPIs to an unhosted wallet at the request of a customer, it is not subject to the Travel Rule. Nevertheless, even for transactions that are not subject to the Travel Rule, information on the counterparty (name, blockchain address, etc.) must be obtained and recorded.

Promotion and testing

On June 15, 2018, the Cabinet Office of Japan announced the "Basic policy for Regulatory Sandbox scheme in Japan". The Regulatory Sandbox is a scheme to introduce new, outstanding technologies, such as AI, IoT, big data and blockchain, in Japan, and encourages new ideas for "test projects" in any industrial sector, whether in or outside Japan.

By utilising this scheme and using sidechain and atomic swap technology, test projects were conducted to establish a platform that enables simultaneous delivery of Crypto Assets and settlement in fiat currency, eliminating credit risks to counterparties. This is part of the efforts to create a market for professional CAESPs to efficiently conduct covering transactions.

Ownership and licensing requirements

There is no restriction on an entity simply owning cryptocurrencies for its own investment purposes, or investing in cryptocurrencies for its own exchange purposes. As a general rule, the Crypto Asset regulations under the PSA will not be applicable unless an entity conducts CAES as a business. Please note, however, that the sale of certain types of tokens may be subject to regulation under the PSA or the FIEA, as applicable, as discussed in "**Sales regulation**" above.

Mining

The mining of cryptocurrencies is not regulated. Mining in itself does not fall under the definition of CAES. It should be noted, however, that if the mining scheme is formulated as involving CISIs and includes the sale of equity interests in an investment fund, it will be subject to the relevant FIEA regulations.

Border restrictions and declaration

Border restrictions

Under the Foreign Exchange and Foreign Trade Act of Japan, if a resident or non-resident has received a payment exceeding JPY30 million made from Japan to a foreign country or made from a foreign country to Japan, the resident or non-resident must report it to the Minister of Finance. If a resident has made a payment exceeding JPY30 million to a non-resident either in Japan or in a foreign country, the same reporting requirement applies.

On May 18, 2018, the Ministry of Japan announced that the receipt of payments in Crypto Assets or the making of payments in Crypto Assets, the market price of which exceeds JPY30 million as of the payment date, must be reported to the Minister of Finance.

Declaration

There is no obligation to declare cryptocurrency holdings when passing through Japanese Customs.

Reporting requirements

As explained above, a certain payment or receipt of payment exceeding JPY30 million, either by fiat currencies or Crypto Assets, is subject to a reporting obligation to the Minister of Finance under the Foreign Exchange and Foreign Trade Act.

A CAESP must report to the relevant authority if it detects a suspicious transaction.

Estate planning and testamentary succession

There has been no established law or court precedent with respect to the treatment of cryptocurrencies under Japanese succession law. Under the Civil Code of Japan, inheritance (i.e., succession of assets to heir(s)) occurs upon the death of the decedent. Theoretically, cryptocurrencies will be succeeded to by heir(s). However, given the anonymous nature of cryptocurrencies, the identification and collection of cryptocurrencies as inherited property would be a material issue unless the relevant private key or password is known to the heir(s). On the other hand, even if the private key or password is unknown, to the extent that the inherited property can be identified, theoretically, inheritance tax may be imposed. An enclosed and notarised testament may be one of the solutions for these issues. However, from the perspective of Japanese law, the legal framework must be improved so that these new issues can be adequately dealt with.

Takeshi Nagase
Tel: +81 3 6775 1200 / Email: takeshi.nagase@amt-law.com

Takeshi Nagase is a fintech partner at Anderson Mōri & Tomotsune. He handles finance and corporate transactions, and has considerable experience advising on all legal aspects of public and private mergers and acquisitions, joint ventures, fintech (including, among others, Crypto Asset regulations, and regulatory requirements for registration of CAESPs, initial coin offerings, and the like), and other corporate and financial advisory matters. His clients range from prominent financial institutions to Crypto Asset start-ups. Between 2013 and 2014, Takeshi served on secondment in the disclosure department of the Financial Services Agency of Japan, where he was an instrumental part of the team that revised the laws and guidelines governing disclosure by listed companies, and prepared the Japanese Stewardship Code. Additionally, he handled a broad range of finance and corporate transactions on a secondment stint with the legal department of a major Japanese securities firm from 2015 to 2017. As a result of the unique perspective he has gained from these professional experiences, Takeshi is often sought for his advice on finance-related matters, particularly by clients seeking to evaluate transactions from the regulator's point of view.

Takeshi also serves as legal advisor to the NFT subcommittee of the Japan Cryptoasset Business Association, one of the largest blockchain industry associations in Japan.

Takato Fukui
Tel: +81 3 6775 1207 / Email: takato.fukui@amt-law.com

Takato Fukui is a partner at Anderson Mōri & Tomotsune. Based on his experience at the Financial Services Agency of Japan and the Japan Virtual and Crypto Assets Exchange Association, Takato advises fintech companies and financial institutions on fintech legal issues, including those of Crypto Assets.

Keisuke Hatano
Tel: +81 3 6775 1250 / Email: keisuke.hatano@amt-law.com

Keisuke Hatano is a partner at Anderson Mōri & Tomotsune. Keisuke specialises in payment and settlement-related regulations. He has also been involved in a number of significant finance transactions, including representing clients in many international and domestic litigations on finance-related matters, among others. During his time at Anderson Mōri & Tomotsune, he was also seconded to the Financial Services Agency of Japan, where he was an instrumental part of the team tasked with making significant amendments to the Banking Act with the aim of facilitating a pro-fintech ecosystem and environment in Japan.

Anderson Mōri & Tomotsune

Otemachi Park Building, 1-1-1 Otemachi, Chiyoda-ku, Tokyo 100-8136, Japan
Tel: +81 3 6775 1000 / URL: www.amt-law.com

Liechtenstein

Matthias Niedermüller & Giuseppina Epicoco
Niedermüller Attorneys at Law

Government attitude and definition

Introduction

Liechtenstein is, in general, a very crypto-friendly jurisdiction. The Liechtenstein government recognised very early on the advantages and potential of blockchain and distributed ledger technology ("**DLT**") as well as the need and market demand for regulation in this area. In early 2018, the government therefore installed a work group with the task of providing a comprehensive and sustainable legal framework for long-term regulation of aspects of blockchain technology. At the beginning of 2019, proposals for the Blockchain Act were discussed and in autumn 2019, a law was passed in Parliament and entered into force in January 2020. The Blockchain Act (officially known as the Law on Tokens and Trusted Technology ("**TT**") Service Providers, or "**TVTG**") provides a comprehensive and technology-neutral approach to regulating the entire token economy. On the one hand, it regulates the rights and obligations of certain clearly defined service providers who perform activities on TT systems. They are subject to license and supervision by Liechtenstein's Financial Market Authority ("**FMA**"). On the other hand, the TVTG creates a new civil law for cryptoassets and the legal basis for the ownership, possession, and disposition rights over cryptoassets. By also regulating the civil law aspects of cryptoassets in a so-called Token Container Model ("**TCM**"), Liechtenstein took a pioneering role in the EU and thus created the first comprehensive legal framework and legal certainty for the tokenisation of "real-world assets". Also, the TVTG partly acted as a role model for regulation at EU/EEA level.

The government and the FMA as the competent regulator generally take a progressive and open approach to cryptoassets and the blockchain space in general and provide substantial support to enable the building of a token economy. The government with the Office for Financial Market Innovation and the FMA with the Regulatory Laboratory and Department for Finance Innovation created their own departments that are dedicated to dealing with fintech and innovation in the financial markets in general.

Liechtenstein's continued open and progressive approach has received substantial attention in international media and also led to an ongoing interest in setting up new blockchain-related businesses in Liechtenstein. Besides the regulatory aspects and flexible corporate law, an attractive tax regime as well as the unique parallel access to the EU, EEA and Swiss markets are considered decisive factors for setting up new businesses in Liechtenstein. Furthermore, the small size of the country generally provides flexibility and short decision-making paths.

MiCA

It is well known that the Markets in Crypto-Assets Regulation ("**MiCA**") entered into force on 29 June 2023 and will become applicable after a transition period of 12 or 18 months. Given that Liechtenstein is an EEA Member State, MiCA will also be applicable in

Liechtenstein and will replace the provisions of the TVTG. In order to provide for a smooth transition from the TVTG regime to the MiCA regime and also for the grandfathering of existing licences, the Liechtenstein government has decided to adjust the TVTG regulations. Thus, companies that have already registered under the provisions of the TVTG prior to the expiry of the transition period will have the opportunity to obtain a licence under MiCA in a simplified and accelerated procedure and then benefit from EU-wide passporting once MiCA is in force.

However, MiCA does not include any regulations on the civil law aspects of cryptoassets or tokens. It is therefore entirely at the discretion of each EU Member State to establish a corresponding legal basis. As mentioned, the TVTG already provides a comprehensive civil law basis for the creation, ownership and transfer of cryptoassets. This part of the TVTG will remain in force for all cryptoassets even after MiCA comes into force in Liechtenstein, irrespective of whether they are covered by MiCA or not.

Cryptocurrencies are not legal tender

In Liechtenstein, cryptocurrencies do not qualify as legal tender. Consequently, cryptocurrencies are not considered "money" in a narrow sense. Depending on the specific design of the cryptoasset, it may be qualified as e-money under the Liechtenstein E-Money Act ("**EGG**").

Although cryptocurrencies do not qualify as legal tender, some cryptocurrencies such as Bitcoin and USDC/USDT are already widely accepted as means of payment by enterprises and shops. From a tax perspective, Bitcoin is also considered foreign currency. The Liechtenstein tax authority publishes exchange rates between several common cryptocurrencies (Bitcoin and Ethereum) and the Swiss franc ("**CHF**") for tax purposes. Cryptocurrencies are also accepted by the Ministry of Justice to provide initial capital contribution for the formation of legal entities. Furthermore, the Liechtenstein government is also planning to accept Bitcoin as payment for government services (e.g., taxes).

Liechtenstein has strong treaty ties to the economic and currency areas of Switzerland. Liechtenstein and Switzerland are a monetary union, which means that CHF is the legal tender of Liechtenstein and that the Swiss National Bank ("**SNB**") serves as the central bank for Liechtenstein. The SNB has not issued any central bank cryptocurrencies (digital currency) like an e-Swiss franc. Also, the Liechtenstein government has not yet issued any cryptocurrency. Therefore, there is currently no form of "state-backed" cryptocurrency available in Liechtenstein.

Cryptocurrency regulation

Crypto services to end users are not expressly prohibited under Liechtenstein law. Liechtenstein law does not provide restrictions on owning and using cryptocurrencies for transactions. Also, exchange between fiat currencies and cryptocurrencies is permitted. Even official authorities accept payments in some cryptocurrencies and the registered capital for formation of entities may be provided in cryptocurrency.

However, providing services related to cryptocurrencies on a commercial basis is subject to licensing to some extent. Liechtenstein has a legal framework regulating the entire life cycle of cryptoassets of all kinds through the TVTG[1] and the Ordinance on the Token and Trusted Technology Service Provider Act (also known as the Blockchain Ordinance, or "**TVTV**").[2] This framework has been in force since January 2020. Furthermore, the FMA published Guideline 2020/1[3] in which some licensing aspects are outlined in more detail.

The TVTG implemented rules for the legal nature of cryptoassets, the basis in terms of civil law with regard to cryptoassets and the representation of rights through cryptoassets and their transfer (Art. 3-10 TVTG) and certain licensing requirements for the provision of professional blockchain-related services (Art. 11-38 TVTG).

As mentioned, the TVTG defines and regulates certain services in connection with DLT, which may only be provided after licensing with the FMA. The services defined and regulated are as follows:

- *Token Issuer*: a person who publicly offers tokens in their own name or in the name of a third party (for example, an exchange that conducts an initial coin offering ("**ICO**") for a third party) (there is an exemption from the licensing requirement for ICOs of less than CHF 5 million within 12 months – see below for detail on the licensing obligation after the amendment of the TVTG).
- *TT Key Depository*: a person who safeguards private keys for third parties) (i.e., Crypto Custodian).
- *TT Token Depository*: a person who safeguards tokens in the name of and on account of others (i.e., Crypto Custodian).
- *Exchange Service Provider*: a person who exchanges legal tender for tokens and *vice versa* as well as tokens for tokens).
- *TT Identity Service Provider*: a person who identifies the person in possession of the right of disposal related to a token and records it in a directory.
- *TT Price Service Provider*: a person who provides TT system users with aggregated price information on the basis of purchase and sale offers or completed transactions.
- *TT Protector*: a person who holds tokens on TT systems in their own name on account for a third party.
- *TT Verifying Authority*: a person who verifies the legal capacity and the requirements for the disposal over a token.

A person that provides at least one of the above services is a so-called TT service provider. TT service providers have to comply with a list of general requirements as well as any additional requirements that apply to the specific services they provide. The regulatory requirements relate to, among other things:

- the initial capital (not applicable for all TT service providers);
- the IT infrastructure;
- the corporate structure/organisational requirements; and
- the suitability of management.

The civil law aspects of the TVTG regulate the rules for the creation, ownership, transfer and deletion of a cryptoasset and therefore its entire life cycle. One of the unique aspects of the TVTG is that it defines the civil law aspects of all possible cryptoassets using a TCM. The TCM defines a token from a civil law aspect as a legal instrument. Under the rules of the TVTG, a token is considered a container of rights that may contain any kind of right or claim. The TCM also means that the rights contained in a token are not directly affected or altered in nature and can be either subject to Liechtenstein law or any other foreign law. Due to the legal design and concept as a container of rights, the token can therefore be applied invariably and used as the bearer of any kind of rights with regard to any kind of asset.

As mentioned above, Liechtenstein is in the process of adjusting the TVTG to ensure a smooth transition to MiCA. The main changes are the alignment of the existing TVTG terminology with MiCA; e.g., the definition "cryptoasset" will be included in the TVTG and will partially replace the "token" definition. Furthermore, cryptoasset services such

as "operating a trading platform", "providing advice on cryptoassets", "providing portfolio management on cryptoassets" and "providing transfer services for cryptoassets on behalf of clients" will be included in the TVTG. Relevant regulations for service providers already subject to licensing under the TVTG, which will also be later subject to licensing under MiCA, such as providing cryptoasset custody and administration services (TT Key Depositories and Token Depositories), exchanging cryptoassets for funds or other cryptoassets (Exchange Service Providers) as well as placing of cryptoassets (Token Issuers for third parties) will be aligned with MiCA so that there is a consistent regulation standard for the transitional period. In addition, the licensing obligation for Token Issuers who publicly offer cryptoassets in their own name will also be entirely removed and, in accordance with MiCA provisions, they will only be obliged to publish a whitepaper (known as a Basic Information Document, or "**BID**" in Liechtenstein).[4]

Other regulations

Depending on the qualification of the respective cryptoasset (for instance, a security token), further financial market rules and licensing requirements may apply, such as those under the Banking Act, the EGG, the Act on Alternative Investment Funds (e.g., crypto funds) or the EU Prospectus Regulation (e.g., security token offerings ("**STO**") or crypto exchange-traded products ("**ETPs**")).

Sales regulation

In the legislative procedure for the TVTG, it was made clear that financial market regulation as securities and commodities law is technology-neutral and, for this reason, can also apply to regulated activities on DLT. It was stated in detail that the area of application of the financial market regulation is connected in many cases to terms such as legal currency, securities, and financial instruments. It is therefore clear that all cryptoassets representing currencies, securities or financial instruments are also to be classified as such in accordance with financial market regulation.[5] Furthermore, it was made clear that if a service provider also includes services that fall under other financial market laws pursuant to the TVTG, then these laws are applicable in addition to the TVTG.

The sales regulations can be summarised as follows.

Security tokens

All tokens that contain rights that qualify them as financial instruments under the regulations of the Markets in Financial Instruments Directive ("**MiFID II**") as defined in the Banking Act are considered security tokens. Hence, the rules applicable to the specific financial instrument are also applicable to such security tokens. In particular, rules regarding public offering, listing on exchanges, trading, etc., are applicable. In this regard, particularly for public offerings of security tokens, the EU Prospectus Regulation and the national implementing laws have to be followed. According to these rules, the public offering and hence the selling of security tokens are regularly subject to prospectus requirements if the relevant thresholds are met. Liechtenstein, unlike several other countries, made use of the possibility to allow public offerings of financial instruments without prospectus requirements up to an amount of CHF 8 million for national offerings. Furthermore, in any event, private placements are exempted from the prospectus requirements. In addition, it has to be noted that security tokens (e.g., shares, bonds, derivatives) must only be traded on a licensed multilateral trading facility ("**MTF**"). The provision of such services as an MTF requires a licence as an investment firm under the Banking Act and the exemption under the EU DLT Sandbox Regime of the DLT Regulation (see "Promotion and testing" below).

Payment tokens

Payment tokens are tokens that are accepted to fulfil contractual obligations and therefore replace legal tender in this respect. Basically, payment tokens do not fall under financial market regulation in Liechtenstein. However, if they are widely accepted as a means of payment in return for goods or services and therefore constitute e-money, an e-money licence will be required. Therefore, companies wishing to issue and sell payment tokens that can be qualified as e-money must obtain a licence as an e-money institution from the FMA prior to commencing business.

Utility tokens

All tokens that do not qualify as financial instruments (security tokens) or as payment tokens are considered utility tokens. Typical utility tokens have certain functionalities (in game currencies, etc.) that can be compared with digitalised vouchers. They do not fall under MiFID II regulations or any other financial regulation. However, like for all tokens, the rules of the TVTG apply. According to the TVTG, Token Issuers who issue or sell tokens in their own name or in the name of a client in the amount of CHF 5 million or more within a period of 12 months are obliged to obtain a licence under the TVTG. As mentioned above, with the amendment of the TVTG, the licensing requirement under the TVTG will no longer apply and, in accordance with the provisions of MiCA, Token Issuers who offer and sell tokens in their own name will only be required to publish a whitepaper (or BID).

Stablecoins

Stablecoins are tokens that are fully backed by a set of fiat currencies or other valuable assets and are bound to one or more fiat currency. In this sense, a stablecoin is equivalent to a currency unit, and its aim is to achieve the lowest possible volatility. Each issued stablecoin is secured with the same amount of the currency unit. Thus, depending on the amount of the currency unit received, the same amount of stablecoins is issued. Stablecoins are currently not regulated separately under financial market law or the TVTG (this will change when MiCA is implemented in Liechtenstein). However, they may be subject to licensing requirements under the existing traditional financial market laws. The issuing of stablecoins could be considered as issuing of either a security token, and therefore a financial instrument, or a payment token, which can be qualified as e-money. Thus, the rules for public offerings of financial instruments or issuing of e-money will apply (see above).

Taxation

In general, only natural persons resident in Liechtenstein and legal entities with a seat in Liechtenstein are subject to Liechtenstein tax laws. Given the small size of the country and its position as a financial hub, corporate tax laws are more relevant.

In addition, Liechtenstein tax laws take a material approach towards trading with cryptoassets. Depending on the rights contained in the respective cryptoasset and the qualification of the cryptoasset as a utility token, payment token or security token, different tax rules will apply. As Liechtenstein law does not have capital gains tax on profits from trading with participations, profits from trading with security tokens are tax-free in Liechtenstein and no withholding tax applies. Utility tokens are considered regular commodities and trading profits would be considered trading income that is subject to regular taxation (12.5% in net profits for legal entities).

Payment tokens are considered currencies and trading profits are also considered trading income subject to regular taxation.

Money transmission laws and anti-money laundering requirements

The prevention of financial crime and money laundering is one of the key aspects for the sustainable functioning of the Liechtenstein financial market. As an EEA Member State, Liechtenstein was one of the first countries to implement the fifth EU Anti-Money Laundering Directive ((EU) 2015/849 and (EU) 2015/847). Thus, Liechtenstein law also provides for comprehensive and effective know-your-customer ("**KYC**") and anti-money laundering ("**AML**") regulations under the Due Diligence Act, which also applies in particular for offerings of transactions with cryptoassets.

Furthermore, in 2022, MONEYVAL's report following a comprehensive assessment of Liechtenstein confirmed that Liechtenstein has a very effective system for combatting financial crime and money laundering.

KYC/AML regulation

All Token Issuers (regardless of a licensing obligation under the TVTG) and some TT service providers (TT Key Depositories, TT Token Depositories, TT Protectors, Exchange Service Providers and also, after the amendment of the TVG, operators of trading platforms) are subject to the due diligence obligations under Liechtenstein law and must provide for a KYC and AML procedure. Due to a risk-based approach of the entire KYC and AML rules, the Due Diligence Act allows for application of different rules, depending on the investment volumes, overall volumes, involved countries and involved persons, thus making it more effective. For example, Token Issuers must identify all investors that invest more than CHF 1,000 and respect international blacklists and sanction lists. Furthermore, information concerning the source of funds of the respective investors must be collected.

Since the KYC and AML regulations of the Due Diligence Act are generally applicable to professional trading with any kind of cryptoassets, trading with anonymous counterparts is generally excluded (the so-called "travel rule"). However, on a regulated exchange, typically only the Exchange Service Provider has knowledge of both counterparts of a trade whereas the trading parties do not necessarily know the counterpart.

Promotion and testing

Apart from the EU DLT Sandbox Regime, which will be outlined below, there is no specific regulatory sandbox. However, the FMA has a special fintech department responsible for cryptocurrency and blockchain regulation, as well as for regulation of any future fintechs. Additionally, a special government body responsible for the facilitation of fintech and blockchain development has been established (*Stabsstelle für Finanzplatzinnovation und Digitalisierung*, or Office for Financial Center Innovation and Digitization).

EU DLT Sandbox Regime

As part of the digital finance package, the EU recently adopted the so-called DLT Sandbox Regime with EU Regulation 2022/858 ("**DLT Regulation**"), which will enable the operation of DLT-based MTFs and settlement systems for the first time. These regulations finally provide the basis for enabling trading and settlement of tokens that classify as financial instruments under MiFID II (therefore, tokenised securities/security tokens) on a blockchain-based trading facility. The new regime has been set up on a trial basis for six years in an environment of lower regulatory hurdles and thus aims to allow better exploitation of the development potential of DLT, while still preserving certain requirements for transparency and investor protection. On the other hand, limitations with regard to the volume of activities will apply.

The DLT Regulation will also shortly be applicable in Liechtenstein as an EEA Member State. Market participants may already apply to the FMA for inclusion in the Sandbox Regime in order to become exempt from certain regulatory hurdles.

Ownership and licensing requirements

There are currently no specific licensing requirements for an investment advisor or fund manager holding cryptocurrency (until the amendments of the TVTG and MiCA come into force), apart from those set out under general financial market law.

Ownership

The TVTG creates a new civil law for cryptoassets and a legal basis for the ownership, possession, and disposition rights over cryptoassets. Therefore, Liechtenstein has a legal framework and certainty with regard to ownership, possession, and disposition of cryptoassets.

For example, the TVTG stipulates that the private key holder has the power of disposal over the token. The TVTG further assumes that the person possessing the power of disposal over a token also has the right to dispose of the token. For every previous holder of the power of disposal, it is presumed that he was the person possessing the right of disposal at the time of his ownership. Disposal over the token results in the disposal over the right represented by the token (Art. 7 Para. 1 TVTG). If the legal effect described in Art. 7 Para. 1 TVTG does not come into force by law, the person obliged as a result of the disposal over the token must ensure, through suitable measures, that: (a) the disposal over the token directly or indirectly results in the disposal over the represented right; and (b) a competing disposal over the represented right is excluded.

In addition, the person possessing the right of disposal reported by the TT system is considered the lawful holder of the right represented in the token in respect of the obligor. By payment, the obligor is withdrawn from his obligation against the person who has the power of disposal as reported by the TT system, unless he knew, or should have known with due care, that he is not the lawful owner of the right.

Licensing requirements

The rules of the TVTG and TVTV outline the applicable regulation in Liechtenstein for certain service providers in relation to DLT and cryptoassets. As mentioned above, this regulation will be amended shortly to ensure a smooth transition into the MiCA regime and to enable certain service providers (in particular, exchange services, operating trading platforms and those who provide custody and administration of cryptoassets) to obtain a national licence in Liechtenstein, which can be directly passported into the EEA/EU once MiCA becomes applicable. However, the current licence requirements are as follows.

The licensing requirements are linked to the respective service (the service provider is called the "TT service provider"). Thus, the question of whether a licence is required under the TVTG depends on the service provided and not on the type of cryptoasset involved (as opposed to licence requirements in traditional financial market law). So, if a natural person or legal entity based in Liechtenstein is planning to professionally provide one of the above-mentioned services (in particular, custody or exchange services), a licence issued by the FMA is required to provide such service. According to law, authorisation is known as "registration". However, materially, it is a licence that is comparable to other financial market licences with some minor limitations.

TT service providers have to comply with a list of general requirements as well as additional requirements that apply to the specific services they provide.

General requirements that apply for all TT service providers are as follows:

- *Applicant*: the applicant must be a natural or legal person capable of action (Art. 13(1)(a) TVTG) with headquarters or a place of residence in Liechtenstein.
- *Substance*: for licences under the TVTG, the law provides for minimum substance requirements such as separated office space.
- *Reliability*: the members of the governing bodies of a TT service provider, as well as shareholders, owners or partners that directly or indirectly hold more than 10% of the TT service provider, must meet reliability requirements such as clean criminal records, professionally suitable, etc. This is conducted as a limited fit and proper assessment.
- *Technical suitability*: TT service providers must be sufficiently technically qualified for the service that shall be provided. To meet this criterion, a TT service provider may draw on the expertise of a qualified third party based on outsourcing of services. This point in particular is central for Exchange Service Providers and Custodians.
- *Governance*: for TVTG licences, an adequate organisational structure is required that provides for clear responsibilities and reporting lines, procedures for dealing with conflicts of interest and clear outsourcing policies and agreements, if applicable.
- *Internal procedures and (special) control mechanisms*: TT service providers must implement written internal procedures and control mechanisms that are appropriate in terms of the type, scope, complexity, and risks of the TT services provided. This includes ensuring sufficient documentation of these mechanisms (such as an internal control system, or "**ICS**"). An ICS includes all internal company procedures, methods, instruments and measures to protect the interests of the TT service provider, to ensure proper operations, and to guarantee compliance with legal requirements. An effective ICS includes written instructions on workflows, regular process monitoring, and risk management.
- *Financial resources*: the law provides for some minimum capital requirements as outlined above (the below being the most relevant):
  (i) Exchange Service Providers (Crypto Exchange): this depends on transaction volumes. For transaction volumes of CHF 1 million and above, the minimum capital is CHF 100,000.
  (ii) Token Issuers (for third parties): this depends on issuing volume per 12 months. If tokens with a value of between 5 million and 25 million are issued, the minimum capital is CHF 100,000. If tokens with a value of above CHF 25 million are issued, the minimum capital is CHF 250,000.
  (iii) Crypto Custodians (TT Key Custodians and TT Token Custodians): minimum capital of CHF 100,000.
- *KYC/AML*: a TVTG licence also requires fulfilment of all KYC/AML requirements of the Due Diligence Act (policies, due diligence officer, storage). In particular, adequate KYC and AML policies have to be put in place and approved by the FMA. Furthermore, all KYC/AML data needs to be stored in Liechtenstein.

For some TT service providers, a few additional requirements are given. To be licensed as a custodian requires appropriate measures to be put in place to prevent loss of private keys/tokens, and the safekeeping of such keys and tokens needs to be completely segregated from the business assets. Furthermore, measures need to be established to ensure the clear assignment of customer tokens and to ensure the execution of customer orders in line with

agreements. The custodian must also install a Business Continuity Management programme to ensure that services can be maintained in the event of interruptions. Exchange Service Providers must also have suitable internal control mechanisms before starting their activity, ensuring the disclosure of comparable market prices and purchase and sale prices of the traded tokens.

Token Issuers, for example, at the first issuance of a token (primary market), have to prepare a BID (equivalent to the required whitepaper according to MiCA) that outlines the key information on the token issuing. The content of the BID is similar to the summary of a prospectus under MiFID laws.

The FMA is the competent authority for all licences and subsequent supervision under the TVTG. After licensing, the licensing requirements must be fulfilled on an ongoing basis. However, TT service providers are not subject to the same ongoing prudential supervision as licensed financial intermediaries (e.g., periodic external audits, ongoing review of technical suitability), but rather to event-driven or *ad hoc* supervision. The level of protection ensured by supervision differs accordingly from that of a licensed financial intermediary.

Finally, it should be noted that it is a common practice in Liechtenstein that, in the initial phase of a project, a meeting is held with the FMA in which the project and key items are discussed. Generally, the entire licensing process is conducted in close cooperation with the FMA and can therefore be completed more efficiently. The small size of the country once again provides for additional benefits.

Mining

There is no specific regulation of cryptocurrency mining in Liechtenstein. Mining cryptocurrencies in one's own name and on own account does not trigger licensing requirements. However, depending on the business model, professional mining as a service, on behalf of third parties or with certain participation models, may constitute a service under the TVTG or be considered a service that is subject to financial market laws such as the Banking Act, the EGG or the Act on Alternative Investment Funds. Also, prospectus requirements may be triggered.

Border restrictions and declaration

In Liechtenstein, there are no particular border restrictions or declaration requirements that would apply to cryptocurrencies.

Reporting requirements

There is no statutory threshold amount above which the person responsible for due diligence (*Sorgfaltspflichtige*) would have to report a transaction of a customer. Rather, it is based on the ongoing customer risk assessment by the person responsible for due diligence, which provides for thresholds of between CHF 50,000 and 500,000 depending on the risk categorised, but which are not of a binding nature.

Estate planning and testamentary succession

In Liechtenstein, there are no particular estate planning or testamentary succession aspects concerning cryptocurrencies. Accordingly, general civil law rules apply. Of course, however, there may be factual difficulties in terms of actual accessibility of heirs to cryptocurrencies held in self-custody due to password requirements.

Endnotes

1. English version of the Blockchain Act/TVTG: https://www.regierung.li/files/medienarchiv/950-6-01-09-2021-en.pdf
2. English version of the Blockchain Ordinance/TVTV: https://www.regierung.li/files/medienarchiv/950_61_16_03_2020_en_637357617226079994.pdf
3. FMA Guideline regarding the TVTG: https://www.fma-li.li/files/list/fma-wegleitung-2020-1-registrierung-als-dienstleister-nach-tvtg.pdf
4. See in detail: BuA 73/2023.
5. BuA 2019/54, page 42.

Matthias Niedermüller
Tel: +423 236 1015 / Email: mn@niedermueller.law

Dr. Matthias Niedermüller M.B.L.-HSG is the Managing Partner and Founder of Niedermüller Attorneys at Law.

A notable focus of the firm is the area of digital finance, with the firm advising on the setup of a number of significant blockchain infrastructure projects in Liechtenstein. Matthias has particular expertise in fintech and is also experienced in financial market law – from regulatory to transactional matters, Matthias' expertise covers all aspects within the blockchain and DLT sector.

Being known for his creative corporate and asset protection solutions for crypto, blockchain and DLT projects, Matthias is a reliable advisor when it comes to the creation of operational and holding companies to the structuring of optimised crypto foundations.

Within the blockchain community, clients particularly appreciate Matthias' solution-orientated commitment and 24/7 availability as well as the whole authenticity of the firm by highlighting this positively as follows: "The fact that the entire office is fully digitalized increases their efficiency further. Niedermüller Attorneys have one of the most advanced digital setups in Liechtenstein, it is comparable with other large international firms."

Giuseppina Epicoco
Tel: +423 236 1015 / Email: gep@niedermueller.law

Giuseppina Epicoco is a Partner at Niedermüller Attorneys at Law. Giuseppina specialises in financial market and banking law, financial services regulation, corporate and commercial law as well as fintech and blockchain matters.

Niedermüller Attorneys at Law

Werdenbergerweg 11, 9490 Vaduz, Liechtenstein
Tel: +423 222 0750 / URL: www.niedermueller.law

Lithuania

Vladimiras Kokorevas
Gofaizen & Sherle UAB

Government attitude and definition

The government's attitude towards virtual currencies is generally open and favourable, with efforts being made to regulate and monitor virtual currency-related activities. Lithuanian law[1] in the area of prevention of money laundering and terrorist financing (AML law) defines virtual currency as a digital representation of value that does not possess the legal status of currency or money, is not issued or guaranteed by a central bank or any other public authority, is not necessarily attached to a currency, but is accepted by natural or legal persons as a means of exchange and can be transferred, stored, traded, exchanged, invested or used for settlement electronically. The AML law also sets out separate requirements and thresholds for entities conducting initial coin offerings (ICOs), defining an ICO as an offer made for the first time, directly or through an intermediary, by a legal person established in the Republic of Lithuania or a branch established in the Republic of Lithuania of a legal person of an EU Member State or a foreign state to purchase its virtual currencies for funds or other virtual currencies with a view to raising capital or investment.

The Financial Crimes Investigation Service under the Ministry of the Interior of the Republic of Lithuania (FCIS), which, among other things, supervises the activities of virtual currency exchange operators and depository virtual currency wallet operators (VASPs) in relation to the prevention of money laundering and terrorist financing (ML/TF), and the Bank of Lithuania, the country's central bank, which supervises financial market participants, have issued several communications related to virtual currencies, such as warnings,[2,3] instructions[4] and guidelines. One of the Bank of Lithuania guidelines[5] indicates that virtual currencies, depending on their nature, economic functions and rights awarded by them, may be qualified as payment-type, utility-type or investment-type tokens, or hybrid tokens in some circumstances, which have the characteristics of two or more token types.

It should be noted that the Bank of Lithuania has issued LBCOIN, which, according to the Bank of Lithuania, is the world's first blockchain-based digital collector coin. Together with its physical version, LBCOIN was issued on 23 July 2020.[6] However, to our knowledge, the Lithuanian government does not intend to become actively involved in the issuance of virtual currencies and they cannot be used as a means of payment for interactions with public institutions (e.g., payment of taxes, state fees, etc.). Nevertheless, fulfilling payment obligations in virtual currencies is permitted if parties agree on such means.

Cryptocurrency regulation

Financial services regulation

The Bank of Lithuania has expressed its position that there may be cases when virtual currencies may have characteristics of financial instruments and as a result, such virtual

currencies and entities issuing, holding and/or intermediating/carrying out transactions with said virtual currencies may be subject to financial markets legislation (e.g., prospectus and financial/investment services regulatory requirements).[7] In other words, in the Bank of Lithuania's opinion, regulation should be technology-neutral, which means that the application of financial markets legislation should not depend on the actual use of any technology or on its kind.

The Bank of Lithuania has also noted that, generally, financial market participants supervised by the Bank of Lithuania should not participate in activities or provide services associated with virtual currencies. Activities or services associated with virtual currencies include, among other things, setting up funds intended for investment in virtual assets. However, according to the Bank of Lithuania, a licensed management company may set up an investment fund for professional investors that would invest in virtual assets, subject to compliance with applicable requirements and expectations of the Bank of Lithuania.[8]

Also, it should be noted that the European Banking Authority has issued a report on crypto-assets stating that, in certain cases, depending on the specific features of the virtual currency, such currency may qualify as electronic money, and authorisation as an electronic money institution would therefore be required to carry out activities involving electronic money, unless a relevant exemption applies.[9] Moreover, the Bank of Lithuania is of the opinion that electronic money can be issued using blockchain technology, provided that compliance with applicable regulations and the regulator's position is ensured.[10]

For the purposes of this contribution, we have assumed that virtual currencies are not considered financial instruments and do not qualify as electronic money, and that business models do not have the characteristics of regulated financial services (e.g., activities of the management company, crowdfunding platform operators, payment service providers, etc.).

ML/TF prevention regulation

Lithuania has taken a proactive approach to regulating virtual currency-related activities. In addition to transposing the 5th AML Directive[11] into Lithuanian law, Lithuania has also adopted stricter national requirements related to the activities of VASPs, one part of which entered into force on 1 November 2022 and the other part in early 2023. These changes to the national law have been adopted to ensure more efficient regulation of the crypto sector without waiting for the entry into force of the Markets in Crypto-Assets Regulation (MiCA). However, it should be noted that on 4 September 2023, the International Monetary Fund (IMF) published a report in which it stated, among other things, that although recent amendments to the AML law in Lithuania have increased the requirements for entities seeking to register as a VASP, the regulatory framework is not complete.[12] At the time of writing, a draft AML law[13] has been prepared by the Ministry of the Interior of the Republic of Lithuania, the explanatory memorandum of which states that said draft aims, *inter alia*, to strengthen supervision and regulation of the prevention of ML/TF.

In Lithuania, a VASP is either a legal entity established in the Republic of Lithuania or a branch established in the Republic of Lithuania of a legal person of an EU Member State or a foreign state. Currently, the activities of VASPs are not subject to licensing in Lithuania; however, VASPs must undergo a mandatory registration process before engaging in VASP activities. Under the AML law, a legal person or branch must inform the manager of the Register of Legal Entities no later than five working days from the start or termination of VASP activity. By providing this information in notification form, the VASP also confirms that it and its members of management and/or supervisory bodies and the beneficial owners are familiar with and comply with the requirements of legal acts on the prevention of ML/

TF. It should be noted that as of 1 February 2023, the Register of Legal Entities publishes on its website a list of VASPs carrying out the activities of a virtual currency exchange operator[14] and depository virtual currency wallet operator.[15] This brings more transparency to the market of cryptocurrency service providers.

In general, VASPs that have properly notified the Register of Legal Entities about the commencement of their activities and comply with the requirements of legal acts on the prevention of ML/TF are entitled to manage depository virtual currency wallets on behalf of the customers, providing intermediary services related to ICOs and/or services of virtual currency exchange, purchase and/or sale for remuneration. However, VASPs do not have the right to provide any financial services without an appropriate licence and/or authorisation from the Bank of Lithuania. A list of the financial market participants authorised to provide financial services and supervised by the Bank of Lithuania is published on the Bank's website.[16]

In accordance with the AML law, a VASP must meet the following main requirements (including, but not limited to):

- hold a registered share capital of at least EUR 125,000 if it is a legal entity incorporated in Lithuania (e.g., a private limited liability company) that shall carry out VASP activities (previously the requirement for a private limited liability company was EUR 2,500);
- designate a senior employee to organise the implementation of ML/TF prevention measures specified in the AML law and to liaise with the FCIS (AML Officer);
- the AML Officer cannot represent more than one VASP at the same time, except where those VASPs belong to a single group of undertakings;
- if a management board is formed, the VASP must designate a member of the management board to organise the implementation of ML/TF prevention measures specified in the AML law and an AML Officer to liaise with the FCIS;
- appoint a senior manager who must be a permanent resident of Lithuania, as defined under the Personal Income Tax Law of the Republic of Lithuania. The AML Officer may be designated as a senior manager if he/she complies with the requirements applicable to this position;
- the members of the management and supervisory bodies as well as beneficial owners of the VASP must be of good repute (e.g., must not be found guilty of certain crimes defined by the AML law, etc.);
- establish adequate internal policies and internal control procedures for the prevention of ML/TF and for the implementation of international financial sanctions and restrictive measures. The VASP shall review and, if necessary, update the internal control procedures periodically;
- take appropriate measures so that the VASP's relevant employees are aware of the provisions in force on the basis of the AML law (including ongoing training);
- have in place internal systems that enable it to respond rapidly, through secure channels and in a manner that ensures full confidentiality, to FCIS enquiries;
- where the VASP is part of a group of undertakings, as defined by law, it must implement group-wide policies and procedures for the prevention of ML/TF, and also comply with the national legislation of the EU Member State in which the subsidiary or branch is established; and
- not operate or provide services in another state to the extent that only non-essential functions or services would remain in the Republic of Lithuania in accordance with the nature of their activities. While the AML law does not prohibit the acceptance of foreign customers, it specifies that the services shall not be provided in a manner in which they would be performed or provided exclusively to customers of another state.

In the aforementioned instances, in principle, the VASP would no longer carry out activities in the Republic of Lithuania. The purpose of such a requirement is to ensure that the VASP has a real connection to Lithuania and is accountable to Lithuanian supervisory authorities.

Taxation

Lithuania does not have any specific legislative provisions on the taxation of cryptocurrencies, so the usual taxation rules apply. Cryptocurrencies can be classified into different asset classes depending on the applicable tax laws. Generally, individuals and businesses are required to report cryptocurrency-related income and gains for tax purposes. The specific tax rates depend on the type of virtual currency, nature of activities, transactions and other factors. The sale of virtual currency transactions is considered a transaction for the provision of financial services, which is normally exempt from value-added tax.

Money transmission laws and anti-money laundering requirements

The AML law and requirements for obliged entities are applicable to VASPs, requiring them to implement robust procedures to prevent ML/TF and other illicit activities. Below are some additional key anti-money laundering requirements applicable to VASPs, which supplement the requirements mentioned above. It should be noted that this section is not intended to provide an exhaustive list of AML requirements.

Customer due diligence requirements must be applied by VASPs:

- prior to establishing a business relationship;
- before carrying out virtual currency exchange operations or transactions in virtual currency with funds amounting to EUR 700 or more, or the equivalent amount in foreign or virtual currency, or before depositing virtual currency to or withdrawing virtual currency from the depository virtual currency wallet in an amount equal to EUR 700 or more, or the equivalent amount in foreign or virtual currency, whether that transaction is carried out in a single operation or in several operations that appear to be linked (the value of the virtual currency is determined at the time the monetary operation is carried out or the transaction is concluded), except for cases where the customer and the beneficial owner have been already identified;
- when the VASP has doubts about the veracity or authenticity of the previously obtained identification data of the customer and beneficial owner; or
- in any other case, when there are suspicions that an act of ML/TF is, was or will be carried out, regardless of any derogations, exceptions or limits provided for in the VASP's policies and applicable legislation.

The obligation to apply customer due diligence measures includes the following main requirements:

- identification and verification of the customer's (and representative's) identity using documents, data or information from reliable and independent sources;
- identification and taking reasonable measures to verify the beneficial owner's identity so that the VASP is satisfied that it knows who the beneficial owner is, including in the case of a legal entity or trust, measures to enable the VASP to understand the ownership and management structure, as well as the nature of activities of the legal entity or trust;
- identification and taking reasonable measures to verify whether the customer is a politically exposed person (PEP) or a person connected to a PEP (family member, close associate, etc.);

- obtaining information on the purpose and intended nature of the business relationship;
- monitoring of the business relationship (including monitoring of transactions and keeping the customer's data up to date);
- screening the relevant persons against the relevant financial sanctions lists; and
- assessing the ML/TF risks of the customer and assigning them an appropriate risk category.

It is prohibited for VASPs to open anonymous accounts or accounts under obviously fictitious names. The AML law establishes requirements to collect and verify certain data about customers, their representatives and beneficial owners. It also provides alternative options for customer identification procedures in case of remote onboarding of customers, some of which are listed below:

- reliance on a third party in accordance with the procedure provided in the AML law, where the VASP obtains information about the customer and beneficial owner from a third party that is a financial institution, or any other obliged entity registered in an EU or non-EU Member State, meeting the requirements laid down in the AML law;
- use of electronic identification means issued in the European Union that operate under electronic identification schemes with high or substantial assurance levels, as specified by Regulation (EU) 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC; and
- use of electronic means allowing direct video streaming in accordance with the technical requirements established by the FCIS. One method is when the customer's face and the original identification document produced by the customer are captured by way of direct video streaming.

In addition to the aforementioned requirements and obligations, the VASP must also comply with the following:

- Risk-based approach: VASPs shall conduct regular risk assessments of their business activities (including specific products, services, entities, geographic locations) and customers to identify the adequate measures to be applied to prevent or mitigate ML/TF threats.
- Suspicious transaction reporting: If a VASP becomes aware or suspects that another person is engaged in ML/TF, it is obligated to report it to the FCIS as the Lithuanian Financial Intelligence Unit.
- Record-keeping: VASPs must maintain records of transactions within the relevant logbooks, customer data and other information for a specific period of time (five or eight years, depending on the type of information). Time limits for storage may be extended by up to two years upon the reasoned instruction of a competent authority. These records should be easily accessible to regulatory authorities upon request.

As of 1 January 2025, VASPs will also be obliged to apply the Travel Rule, requiring them to collect, store and transmit certain transaction and customer information to the VASP or financial institution of the recipient of the transaction. The VASP itself must not accept a transaction from another VASP if the latter fails to comply with the requirement to transmit the required information.

Failure to comply with these requirements can result in penalties and legal consequences. It is important for VASPs to understand and adhere to the ML/TF prevention regulations and regularly update their compliance procedures as per the evolving regulatory landscape.

Promotion and testing

Lithuania has shown interest in attracting FinTech companies, promoting the development and application of new products based on distributed ledger technology in the financial area and improving regulatory quality.

Calls from the Bank of Lithuania for proposals to create a blockchain sandbox called LBChain were subject to the great initiative and led to the successful launch of the platform after two years of development. The Bank of Lithuania describes LBChain[17] as the world's first-of-its-kind blockchain sandbox developed by a financial market regulator that combines regulatory and technological infrastructures and allows FinTech companies to test their business solutions in a controlled environment. The Bank of Lithuania notes that the platform is aimed at serving the key needs of FinTechs and start-ups and provides them with the possibility to gain new knowledge, carry out blockchain-oriented research, test and adapt blockchain-based services as well as offer advanced innovations to their clients. The Bank of Lithuania acknowledges the lack of general knowledge and experience of start-ups when it comes to the financial ecosystem, legal issues and regulation. In order to help them bring their bold and innovative ideas to life, LBChain offers:

- a state-of-the-art technological testing platform based on Hyperledger Fabric/Corda;
- regulatory support from the Bank of Lithuania;
- technological support from leading blockchain integrators; and
- a cost-efficient and low-risk path to innovation.

Solutions already tested by LBChain include, among others:

- a know-your-customer solution for anti-money laundering compliance;
- cross-border payments;
- a smart contract for factoring;
- a mobile point of sale and payment card solution;
- an unlisted share trading platform;
- a crowdfunding platform; and
- payment tokens.

The Bank of Lithuania notes that even in the development stages, LBChain was used by 11 FinTech start-ups from eight countries testing over 10 different products and services. The potential of the LBChain platform was evidenced in 2020 when it won the national round of the World Summit Awards in the category of "Government and citizen engagement".

Mining

There are no specific regulations for cryptocurrency mining activities in the country. However, it is important to note that the operation of mining facilities may be subject to general regulations regarding electricity consumption, land use, or environmental protection. It is advisable for miners to comply with applicable laws and regulations related to these areas. Also, mining activities in certain cases are subject to taxation.

Border restrictions and declaration

There are no specific border restrictions or obligations to declare virtual currency holdings when entering or leaving Lithuania. In Lithuania, any person carrying cash equal to EUR 10,000 or more (or the equivalent of that sum in other currency) is required to declare that sum at the customs office. Generally, virtual currencies are not considered cash in Lithuania,

especially considering their usual internet-based nature. However, it is essential to stay updated on any changes in regulations or requirements, as cryptocurrency laws and regulations are constantly evolving. It is also worth noting that individuals travelling to other countries should research and comply with the virtual currency regulations of their destination country, as some countries may have specific requirements or restrictions in place.

Reporting requirements

VASPs are required to submit external reports to the FCIS through the AML Officer. Legal acts related to ML/TF prevention and implementation of international financial sanctions require VASPs to submit the reports detailed below. The AML Officer shall have access to the FCIS reporting system through which reports can be submitted. Please note that tax-related reports, declarations, etc. are outside the scope of this chapter and shall not be discussed.

Amount-based reports

Amount-based reports shall be made if a customer makes virtual currency exchange transactions or transactions in virtual currency, if the daily value of such transaction(s) is equal to or exceeds EUR 15,000 or the equivalent amount in foreign or virtual currency, regardless of whether the transaction is concluded in one or more related transactions within a 24-hour period. The report shall be sent to the FCIS no later than seven working days after the execution of the transaction.

Suspicious transaction reports

A VASP shall report to the FCIS transactions whereby the VASP has established that a customer is carrying out a suspicious transaction, the VASP knows or suspects that assets of any value have been obtained directly or indirectly from criminal activity or involvement in such activity, or if the VASP knows or suspects that such assets are involved in terrorist financing. It is important to note that there is no minimal threshold or limit for such a report. Suspicious transactions shall be identified:

- by noting activities of customers that, by their nature, may be related to ML/TF;
- when conducting customer and beneficial owner identification;
- when conducting ongoing monitoring of the business relationship, including the investigation of transactions that have occurred during that relationship; and
- in accordance with the minimal characteristics of suspicious transactions provided in the relevant FCIS order.

The AML Officer plays an active role in the identification and reporting of suspicious transactions. The principal functions of the AML Officer include, in particular:

- reviewing all internal disclosures and exception reports and determining whether it is necessary to report to the FCIS;
- maintaining all records related to such internal reviews;
- providing guidance on how to avoid "tipping off"; and
- acting as the main point of contact with the FCIS, law enforcement, and any other competent authorities in relation to ML/TF prevention and detection, investigation or compliance.

Generally, in the event of an unusual or potentially suspicious transaction, the transaction must be suspended and a documented internal investigation must be carried out. If suspicious activity is detected, a report must be submitted to the FCIS within three working hours of the suspension of a suspicious transaction.

Annual reports

In addition to the above, VASPs must also submit an annual report to the FCIS consisting of information related to the implementation of ML/TF prevention measures. The annual report shall also be submitted by the AML Officer and the deadline for this report is 31 March of each year.

Sanctions

In case of freezing of assets due to international sanctions and restrictive measures, VASPs must inform the FCIS and the Ministry of Foreign Affairs of the Republic of Lithuania thereof within two business days.

VASPs must also inform the FCIS if their owners or participants become subject to financial sanctions, or if they are owned or controlled by entities subject to financial sanctions, within two business days from the date of becoming aware of such information.

Estate planning and testamentary succession

In Lithuania, the treatment of virtual currencies for estate planning and testamentary succession purposes is still a developing area of law. At the time of writing, there are no specific regulations in place that directly address cryptocurrencies in the context of estate planning and testamentary succession.

However, the general principles of Lithuanian inheritance law would apply to virtual currencies as they are likely to be treated as another type of intangible asset, considering that the virtual currency has economic value and can be transferred by the owner to another person. This means that virtual currencies can be included in a person's estate and distributed according to their will or the rules of intestate succession if no will exists.

To ensure the smooth transfer of virtual currencies upon death, it is advisable to include specific provisions in a will or create a separate document that outlines the details of the digital assets and provides necessary instructions for their transfer. It may be helpful to specify the cryptocurrency holdings, addresses of the digital wallets, and any relevant access information to facilitate the transfer of the assets.

* * *

Endnotes

1. Law on the Prevention of Money Laundering and Terrorist Financing of the Republic of Lithuania: https://e-seimas.lrs.lt/portal/legalAct/lt/TAD/TAIS.41300/asr (accessed on 6 September 2023).
2. On 31 January 2014, with regard to the European Banking Authority's (EBA) warning about "virtual currencies", the Bank of Lithuania published its position warning consumers of the potential risks posed by such currencies: https://www.lb.lt/lt/naujienos/lietuvos-bankas-perspeja-del-virtualiu-valiutu-naudojimo (accessed on 6 September 2023).
3. On 16 July 2021, the Bank of Lithuania issued a warning regarding Binance, UAB and other crypto-asset service providers in relation to unlicensed financial activities in Lithuania: https://www.lb.lt/en/news/bank-of-lithuania-issued-warning-regarding-binance-uab-and-other-crypto-asset-service-providers (accessed on 6 September 2023).
4. On 10 January 2020, the FCIS adopted instructions for virtual currency exchange operators and/or depository virtual currency wallet operators (VASPs) aimed at

preventing money laundering and terrorist financing. The FCIS also provides methodological assistance to obliged entities, including VASPs, in the implementation of the anti-money laundering and terrorist financing measures laid down in the AML law.

5. Guidelines of the Bank of Lithuania on security token offering: https://www.e-tar.lt/portal/lt/legalAct/e1018840f18111e99681cd81dcdca52c (accessed on 6 September 2023).
6. Bank of Lithuania website: https://www.lb.lt/en/digital-collector-coin-lbcoin#ex-1-1 (accessed on 6 September 2023).
7. Please see endnote 5.
8. The official position of the Bank of Lithuania on crypto-assets and initial coin offerings: https://www.lb.lt/uploads/documents/files/220127pozicija.pdf (accessed on 6 September 2023).
9. EBA reports on crypto-assets: https://www.eba.europa.eu/eba-reports-on-crypto-assets (accessed on 6 September 2023).
10. FAQs regarding virtual assets and initial coin offerings published by the Bank of Lithuania: https://www.lb.lt/lt/naujienos/lietuvos-banko-pozicija-del-virtualiojo-turto-ir-pirminio-virtualiojo-turto-zetonu-platinimo-atspindi-rinkos-aktualijas (accessed on 6 September 2023).
11. Directive (EU) 2018/843 of the European Parliament and of the Council of 30 May 2018 amending Directive (EU) 2015/849 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing, and amending Directives 2009/138/EC and 2013/36/EU (Text with EEA relevance).
12. Nordic-Baltic Regional Report: Technical Assistance Report-Nordic-Baltic Technical Assistance Project Financial Flows Analysis, AML/CFT Supervision, and Financial Stability: https://www.imf.org/en/Publications/CR/Issues/2023/09/01/Nordic-Baltic-Regional-Report-Technical-Assistance-Report-Nordic-Baltic-Technical-538762 (accessed on 6 September 2023).
13. https://e-seimas.lrs.lt/portal/legalAct/lt/TAP/6d9063a036af11eeb4b9a076396dcf81?jfwid=-1c2mg5vjpc (accessed on 6 September 2023).
14. List of virtual currency exchange operators: https://www.registrucentras.lt/jar/sarasai/vvko.php (accessed on 6 September 2023).
15. List of depository virtual currency wallet operators: https://www.registrucentras.lt/jar/sarasai/dvvpo.php (accessed on 6 September 2023).
16. A list of financial market participants published on the Bank of Lithuania website: https://www.lb.lt/en/sfi-financial-market-participants (accessed on 6 September 2023).
17. Bank of Lithuania on LBChain: https://www.lb.lt/en/lbchain (accessed on 6 September 2023).

Vladimiras Kokorevas
Tel: +370 661 083 08 / Email: vladimiras@gofaizen-sherle.com

Vladimiras Kokorevas, a native of Vilnius, Lithuania, holds a Master's degree in law from the Faculty of Law of Mykolas Romeris University (he completed a double-diploma study programme that Mykolas Romeris University (Lithuania) conducted in cooperation with its study partner, the University of Savoie Mont Blanc (France)). With over six years of experience, Vladimiras has worked extensively as a senior lawyer at various law firms and international companies, including as Chief Legal Counsel at a financial institution.

Vladimiras specialises in the complexities of corporate law, financial services regulation, establishment, licensing and the activities of financial institutions and FinTech companies. In addition, the combination of a Master's education and relevant experience equips him with the competence to excel in the field of anti-money laundering and counter-terrorism financing within the Lithuanian jurisdiction and other European contexts.

Gofaizen & Sherle UAB

Lvivo str. 25-702, Vilnius, Lithuania
Tel: +370 661 083 08 / URL: www.gofaizen-sherle.com

Mexico

Carlos Valderrama & Arturo Salvador Alvarado Betancourt
Legal Paradox®

Government attitude and definition

The Mexican Government has issued regulations applicable to companies that carry out or facilitate the purchase, sale, custody, storage or transfer of virtual assets ("**Transactions with Virtual Assets**") as well as regulations applicable to financial entities.

In said context, it is very important to have a clear distinction between the regulation applicable to non-financial entities and financial entities. The first are those companies that carry out activities, services or operations that are not reserved by financial regulation specifically in favour of any financial entity ("**Non-Financial Entities**"), and therefore their performance does not require prior registration, authorisation or concession by the financial authorities. The latter are those that perform an activity or offer a product or service that is reserved ("**Reserved Activity**") to that type of financial entity by the applicable financial regulation ("**Financial Entities**"), and therefore, in order to perform such activity, it is necessary to obtain prior registration, authorisation or concession from the Ministry of Finance and Public Credit ("**MFPC**"), the National Banking and Securities Commission ("**NBSC**"), the National Insurance and Bonding Commission or the National Retirement Savings System Commission (jointly or separately, "**Financial Authorities**").

This distinction between the regulation applicable to different types of companies regarding activities carried out with virtual assets was born from the publication of the Law to Regulate Financial Technology Institutions in March 2018 ("**FinTech Law**"), which came to reform the Federal Law for the Prevention of Operations with Resources of Illicit Proceeds ("**Anti-Money Laundering Law**") along with another set of regulations. This was the first time in Mexico that regulations were issued regarding operations carried out with virtual assets.

The last regulatory reform on this matter took place on June 7, 2023, when the National Procedures Code was published and, for the first time in Mexico, terms such as "Blockchain" and "Metaverse" were defined at a regulatory level, expressly recognising the evidential value of information, electronic documents or data messages contained or stored in a Blockchain.

Although, in the past, the possibility has been contemplated for parties in a trial to present evidence stored in technological media, for greater validity, it is now required that this type of evidence be presented together with evidence that the information contained in the data message has remained intact and unaltered from the time it was first generated and, in such terms, is accessible for subsequent consultation. For this purpose, it is necessary to comply with the requirements contemplated in Mexican Official Rule NOM-151-SCFI-2016 issued by the Ministry of Economy that establishes the requirements for the digitisation and preservation of such data messages.

The National Procedures Code breaks the previous rule by recognising the existence of information, electronic documents or data messages contained or stored in a Blockchain, as well as conferring full evidence of the type of data contained in a public Blockchain. The fact that it confers full evidence means that, by its mere contribution as proof in court, the related fact is demonstrated. In this sense, it is no longer up to the offeror to prove that the requirements related to the digitisation and preservation of data have been met, but it is up to the counterparty to provide elements to disprove it by demonstrating the violation or manipulation of the information contained in the public Blockchain. In addition, the National Procedures Code became the first Mexican regulation to contemplate the Metaverse as a space for trial hearings.

By way of preamble and subject to further analysis of what the Mexican regulation establishes, it is necessary to mention that neither virtual assets nor any other asset based on blockchain technology is backed by Banco de México, the Mexican Central Bank ("**Banxico**"), nor are they recognised as legal tender.

Cryptocurrency regulation

Except for that related to virtual assets, Mexican regulation does not establish specific treatment for the different types of tokens that may be issued in a Blockchain, such as:

1. Non-Fungible Tokens ("**NFTs**"): cryptoassets that cannot be replaced by others of the same species, quality and quantity. They usually represent digital artworks or collectibles, which may or may not generate the right for the holder to have the graphic representation of the work.
2. Utility Tokens: cryptoassets that provide access to specific functions or services, such as exercising voting rights in a certain community, access to certain benefits such as pre-sales or discounts, entry to events or conferences, among others.
3. Stablecoins: cryptoassets that are designed to mitigate the volatility that exists in other types of assets, with the possibility of being backed 1:1 with fiat currencies.
4. Security Tokens: cryptoassets whose possession gives the holder economic or corporate rights to exercise against the issuer of such asset. These tokens are linked to shares, debentures, bonds, warrants, certificates, promissory notes, bills of exchange or other credit titles, and represent either the capital stock of a legal entity, an aliquot part of an asset or the participation in a collective credit or any individual credit right.
5. Central Bank Digital Currency ("**CBDC**"): cryptoassets issued by central banks to replace traditional fiat currencies.

The FinTech Law defined what should be understood by virtual asset, establishing that it is considered as such ("**Virtual Assets**"):

> "[T]he representation of value registered electronically and used among the public as a means of payment for all types of legal acts and whose transfer can only be carried out through electronic means. In no case will virtual assets be understood as legal tender in national territory, foreign currency or any other asset denominated in legal tender or foreign currency."

Through this Law, it was established that Credit Institutions ("**Banks**"), as well as Financial Technology Institutions ("**FTIs**"), which include Electronic Payment Funds Institutions ("**EPFIs**") and Collective Financing Institutions ("**CFIs**"), as Financial Entities, could enter into transactions with their clients only with the Virtual Assets determined by Banxico.

EPFIs are Financial Entities whose purpose is the issuance, administration, redemption and transmission of electronic payment funds, through any means of electronic or digital communication. Such electronic payment funds are referred to the equivalent of an amount

of money in local currency, foreign currency or a determined number of units of Virtual Assets. In order to operate in Mexico, these types of entities require prior authorisation from the NBSC and its Inter-Institutional Committee, which is a body formed by members of the MFPC, NBSC and Banxico.

On the other hand, CFIs are Financial Entities whose purpose is to put people from the general public in contact with each other, in order to grant debt, equity, co-ownership or royalty financing, through any electronic or digital means of communication, which can also be denominated in local currency, foreign currency or Virtual Assets. Also, in order to operate in Mexico, these types of entities require prior authorisation from the NBSC and its aforementioned Inter-Institutional Committee.

Notwithstanding the permissive rule provided for in the aforementioned FinTech Law, Banxico, in March 2019, through Circular 4/2019, established that neither Banks nor FTIs are authorised to enter into direct Transactions with Virtual Assets with their clients due to their volatility, costs, difficulty of scaling, technological complexity, possible lack of understanding of the risks they represent, as well as the risks they represent in terms of prevention of operation with resources of illicit origin and financing of terrorism, as established by Banxico. By virtue of the above causes, Banxico decided to dictate a "healthy distance" between Virtual Assets and the Mexican financial system. Therefore, Financial Entities may not carry out Transactions with Virtual Assets with their customers.

It is worth mentioning that, through the same Circular, Banxico established an authorisation procedure to be followed by the aforementioned entities that intend to carry out internal operations with such assets, provided that no risk is transferred to the client or end user in such operation. As far as we know, no authorisation has been issued for these internal operations; however, if issued, each authorisation will be effective only and exclusively in favour of the entity that has requested it.

Although Banxico has not currently authorised any Financial Entity to execute or facilitate Transactions with Virtual Assets with its clients by virtue of the provisions set forth in the aforementioned Circular, the FinTech Law establishes some minimum disclosure requirements. In this regard, Banks or FTIs that operate with Virtual Assets in the future – as long as Banxico modifies its criteria – must disclose to their clients the risks that exist for carrying out operations with those assets, which must include informing them simply and clearly: (i) that the Virtual Asset is not legal tender and is not backed by the Federal Government; (ii) the impossibility of reversing the operations once executed; (iii) the volatility of the value of the Virtual Asset; and (iv) the technological, cyber, and fraud risks inherent to Virtual Assets.

However, it is worth mentioning that the regulations that apply to the aforementioned Financial Entities do allow them to carry out operations with foreign currency. Could Bitcoin be deemed a foreign currency considering that countries such as El Salvador or the city of Lugano, Switzerland have recognised it as legal tender and, in some cases, such tokens have even been backed by central banks? As of today, neither the Financial Authorities nor Banxico have issued a definitive criterion.

According to Circular 4/2019, in Mexico, those who can directly offer their clients or users Transactions with Virtual Assets are the aforementioned Non-Financial Entities. If Banxico, through said Circular, had recognised any Virtual Asset, the effect would have been the opposite, and only Banks and FTIs could offer their clients transactions with such Virtual Assets and not Non-Financial Entities.

Non-Financial Entities that carry out or facilitate Transactions with Virtual Assets, better known by the Financial Action Task Force ("**FATF**") as Virtual Asset Service Providers, are regulated by the Anti-Money Laundering Law, its Regulations and General Rules that emanate from such Law (jointly, the "**Anti-Money Laundering Legal Framework**").

It is worth mentioning that, in August 2021, the Financial Intelligence Unit ("**FIU**") established, in accordance with international standards on the matter, that Non-Financial Entities engaged in carrying out Transactions with Virtual Assets with their clients in national territory, even if they are incorporated abroad or the technological infrastructure that allows the performance of such operations is located there, are also obliged to comply with the Anti-Money Laundering Legal Framework.

In April 2022, Banxico's current Governor, Victoria Rodríguez Ceja, announced that Banxico's digital currency will start operating in 2025 as part of the long-term payments strategy. It will be interesting to see the development that the Mexican CBDC is going to take.

Sales regulation

Under current regulations, the only express treatment that currently exists is in relation to Virtual Assets. The legal regime to which other types of cryptoassets are subject will depend on the legal nature given to them as a result of an exercise of interpretation of traditional regulation:

1. Virtual Assets: according to the definition analysed above, as long as the corresponding tokens are used as a means of payment, they will be considered Virtual Assets. In this regard, the performance of Transactions with Virtual Assets by Non-Financial Entities could be considered a vulnerable activity in terms of the Anti-Money Laundering Legal Framework (see "Money transmission laws and anti-money laundering requirements" below for information related to the existing obligations on the matter).
2. NFTs: in principle, this type of asset may be the subject of any agreement without its issuance and commercialisation being considered a Reserved Activity. Notwithstanding the foregoing, it is important to consider what will be incorporated in the NFT in order to determine the applicable legal framework in relation to its issuance and commercialisation. For example, if what is incorporated in the NFT is a work of art, its commercialisation could be considered a vulnerable activity in terms of the Anti-Money Laundering Legal Framework, subject to compliance with the obligations on the matter.

   Notwithstanding the foregoing, it will be necessary to consider the specific rights that its possession entails in order to analyse whether it could meet the definition of Security in accordance with the Securities Market Law ("**SML**"). In this case, its issuance and commercialisation will be subject to the fulfilment of the requirements set forth in the SML and its secondary provisions. (For further details, please refer to point 5 of this section.)
3. Utility Tokens: in principle, this type of asset may also be the subject of any agreement without its issuance and commercialisation being considered a Reserved Activity. As for NFTs, it is important to consider what will be incorporated in the token in order to determine the applicable legal framework in relation to its issuance and commercialisation. For example, if what is incorporated in the Utility Token is any type of voucher or games with bets, contests or raffles, its commercialisation could be considered a vulnerable activity in terms of the Anti-Money Laundering Legal Framework, subject to compliance with the obligations on the matter.

   It will be necessary to consider the specific rights that its possession entails in order to analyse whether it could meet the definition of Security in accordance with the SML.

In this case, its issuance and commercialisation will be subject to the fulfilment of the requirements set forth in the SML and its secondary provisions. (For further details, please refer to point 5 of this section.)

4. Stablecoins: the issuance and commercialisation of this type of cryptoasset could be considered a Reserved Activity. As mentioned, with the publication of the FinTech Law, new Financial Entities were created, including EPFIs. As anticipated, these new Financial Entities have the possibility of receiving funds from the general public so that their customers can deposit them in the electronic payment fund accounts – offered by these entities – in order to be able to make transactions in them (such as transfers, payments with cards, and money transmission).

   In this sense, EPFIs receive a certain amount of money from their clients and issue the equivalent in electronic payment funds in the corresponding account. In summary, the electronic payment funds issued turn out to be a payment obligation payable by the corresponding EPFI, similar to the Stablecoin issuance scheme.

   In fact, this same analysis was made by the MFPC, NBSC and Banxico, so they issued a joint communication on June 28, 2021 in which they mentioned that Stablecoins "are units of monetary value that are stored digitally in non-centralized registries (Distributed Ledger Technology) ... a digital unit of value that is associated to the value of a fiat currency". Taking this into consideration, the aforementioned Financial Authorities concluded that the issuance of these cryptoassets is a Reserved Activity to the Financial Entities of the country.

   It should be noted that the type of communication discussed above has no legal binding and although it is a point of reference to know the position of the authority in relation to a certain subject, it does not define the legal treatment that a certain business model with its particularities should receive, in addition to the fact that the subscribed position derives from a value judgment issued by the officials who, at the time, were the heads of the corresponding administrative areas and who are no longer so today. However, it should be noted that the exercise of this activity without the corresponding authorisations may entail the risk of administrative fines and imprisonment.

5. Security Tokens: the current SML establishes that a Security shall be understood as:

   > "[S]hares, partnership interests, debentures, bonds, warrants, certificates, promissory notes, bills of exchange and other *credit titles*, named or unnamed, whether or not registered in the National Securities Registry, susceptible of circulating in the securities markets referred to in the SML, which are *issued in series or masse* and *represent the capital stock of a legal entity, an aliquot part of an asset or the participation in a collective credit or any individual credit right*." [emphasis added]

   In cases where the token to be issued meets the characteristics of the above definition, it will be necessary to comply with the requirements set forth in the SML and its secondary provisions.

   In this regard, the SML provides two types of issuances, according to which specific conditions and requirements must be met in order for the Securities to be legally placed in the national territory:

   a. Private offering of Securities: private offering for the placement of Securities in the national territory must be directed to a closed number of people through a specific investment invitation. For this type of offering, the SML establishes mainly that:
      i. the participation of a third party acting as an intermediary is not required (brokerage firms, Banks, investment fund operating companies, investment fund share distribution companies or retirement fund administrators);

ii. the Securities do not need to be registered in the National Securities Registry;
iii. in the event that the Securities represent the capital stock of legal entities (shares or partnership interests), their offering must be made to less than 100 persons; and
iv. for other types of Securities, their offering must be made exclusively to institutional or qualified investors.

b. Public offering of Securities: public offering for the placement of Securities in Mexican territory is that made through mass media and to an undetermined person. In order to carry out this type of offering, the following requirements must be met:
i. obtain prior authorisation issued by the NBSC;
ii. registration of the corresponding documents in the National Securities Registry;
iii. deposit the corresponding instruments in a Securities Depository Institution;
iv. carry out the listing procedure before a Stock Exchange;
v. place (market to the general public) the Securities through a securities market intermediary (brokerage firms, Banks, investment fund operating companies, investment fund share distribution companies or retirement fund administrators); and
vi. operate under the capital regime of *Sociedad Anónima Promotora de Inversión* (S.A.P.I.), *Sociedad Anónima Promotora de Inversión Bursátil* (S.A.P.I.B.) or, in case the Securities represent the capital stock of the issuing legal entity, under the regime of *Sociedad Anónima Bursátil* (S.A.B.).

The above was recognised in another joint communication dated December 13, 2017 issued by the MFPC, NBSC and Banxico. Through this joint communication, the aforementioned Financial Authorities established that these tokens may meet the characteristics of Securities in accordance with the SML, stating that, if so, their offer to the public would be subject to the conditions and limitations established in said law. As previously indicated, this type of communication has no legal binding and although it is a point of reference to know the position of the authority in relation to a certain subject, it does not define the legal treatment that a certain business model with its particularities should receive. However, it should also be noted that conducting a public offering of Securities without the prior authorisation of the NBSC or conducting a private offering of Securities in violation of the requirements set forth in the regulations may result in the imposition of administrative fines and imprisonment.

Taxation

As of today, according to Mexican tax regulations, there is no specific regime on which taxes must be paid by those who carry out Transactions with Virtual Assets, nor by companies engaged in offering their clients the performance of such operations.

In view of the above, the general principle applicable in Mexico is that all persons in Mexico – whether individuals or companies – are obliged to contribute to the public expense, in accordance with the respective laws, among which are the Income Tax Law ("**ITL**") and the Value-Added Tax Law.

Income tax is a direct tax levied on income received by individuals or legal entities, residents in Mexico and residents abroad with or without a permanent establishment in Mexico. This tax is calculated by applying a rate of up to 35% (for individuals) or 30% (for legal entities) to the taxable income determined in accordance with the parameters of such law.

The legislation that regulates this tax establishes different income accrual and deduction assumptions. The ITL establishes that the corresponding rate must be applied to the corresponding result for the calculation of the tax.

Value-added tax, as an indirect tax, is levied on the consumption of goods and services in different areas, such as the sale of goods, the rendering of services, the granting of the temporary use of goods and the importation of merchandise. Currently, this tax is levied at a general rate of 16% on the values that, in each case, are established to calculate the tax. This tax is owed to the person who performs the aforementioned activities, who must transfer and collect it from the person who acquires the good or service, or from the lessee, as the case may be.

Given the uncertainty of the obligations to which taxpayers who buy or sell Virtual Assets were subject, as well as the exponential growth that the use of this technology has had in Mexico, on November 4, 2021, the Taxpayers' Defense Office issued a criterion to define the regime under which individuals who carry out the sale of Virtual Assets must pay taxes.

Through the aforementioned document, the ombudsman considered that, in tax matters, the profits obtained from the sale of Virtual Assets could not be attributed the tax treatment of an exchange gain as it occurs in the case of foreign currencies. It should be recalled that by that time, El Salvador had already recognised Bitcoin as legal tender.

As a consequence of the above, the ombudsman considered that the tax treatment that should be applied is that of the sale of goods. According to this regime, some of the obligations provided for on this matter are as follows:

1. Withholdings and provisional income tax payments must be made to the Tax Administration Service ("**TAS**") in operations carried out for more than approximately US$13,324.
2. The provisional payment to be made to the TAS shall correspond to the amount resulting from applying a rate of 20% to the total amount of the disposal transaction of the corresponding Virtual Asset.
3. The amount resulting from applying the rate indicated in the preceding point must be given to the TAS by the acquirer of the Virtual Asset, in case the latter is a resident in Mexico or abroad with a permanent establishment in Mexico.
4. In the event that the acquirer does not comply with the conditions indicated in the preceding point, it will be the transferor who will submit the resulting amount to the TAS.
5. The electronic invoice must be issued by the person who carries out the respective sale and in favour of the acquirer. The generic Federal Taxpayers' Registry ("**FTR**") code must be used when the transferor does not have the FTR code of such purchaser.
6. The corresponding income must be incorporated in the annual tax return to be filed, with the transferor having the right to deduct the updated cost of acquisition of the Virtual Asset, as well as any commission that the platform may have charged for the performance or facilitation of the transaction as long as said platform issues the electronic invoice in compliance with the corresponding requirements.

A final point to consider is the tax regime aimed at digital platforms, which applies to persons who obtain income from providing services or selling goods through digital platforms. Basically, it is the digital platform that must make the income tax withholding payments, applying the rates referred to in Section III, Chapter II, Title IV of the ITL, and it will be the same platform that will pay the withholdings directly to the TAS.

Money transmission laws and anti-money laundering requirements

Banks and FTIs do not apply measures for the prevention of money laundering and financing of terrorism related to Transactions with Virtual Assets, since they are not allowed to enter into such operations with their clients or users, as established in the aforementioned Circular 4/2019 issued by Banxico (for further reference, see "Cryptocurrency regulation" above).

Notwithstanding the foregoing, in Mexico, in compliance with FATF Recommendation 15, the Anti-Money Laundering Legal Framework, which applies to Non-Financial Entities that offer or facilitate to their clients the execution of Transactions with Virtual Assets, mainly obliges them to:

1. Presentially apply for registration with the TAS.
2. Once the registration is obtained, enrol in the Money Laundering Prevention Portal administered by the TAS ("**Internet Portal**").
3. Have a Manual containing the policies, criteria, measures and procedures to be adopted by the corresponding company in order to comply with its obligations in terms of prevention of money laundering and financing of terrorism.
4. Designate a Compliance Officer before the Internet Portal, for which, according to the current regulation, obtaining certification granted by the FIU is not mandatory.
5. Apply customer and controlling beneficiary identification policies complying at a minimum with the requirements established by the MFPC, and perform an annual update of the information contained in the respective file.
6. Keep the information and documentation provided by clients and users, as well as that derived from the performance of their operations, for at least five years.
7. Submit notices to the FIU through the Internet Portal containing, as the case may be, information of clients who, within one month or in the accumulated of the last six months, have made purchase or sale operations of Virtual Assets for more than the equivalent of 645 measurement and updating units (as of today, approximately US$3,904.14).
8. Submit notices to the FIU through the Internet Portal, within 24 hours, containing, as the case may be, information on an act or operation that was carried out that has exceeded the threshold established in the preceding paragraph, if the company has information based on facts or indications that the assets or resources could come from or be destined to favour, provide aid, assistance or cooperation of any kind for the commission of a crime of operations with resources of illicit origin or those related to it.
9. Verify and screen against the list issued by the FIU that contains the names of persons identified by national authorities, as well as international organisations or authorities of other countries with which the Mexican Government maintains an international treaty, who are linked to crimes of operations with resources of illicit proceeds or financing of terrorism. In case of a match derived from the screening, within 24 hours after the information is known, a notice must be sent to the FIU, through the Internet Portal, containing the respective client's information.
10. Provide the information required, if applicable, by the MFPC, TAS, FIU or other competent authorities.

Promotion and testing

In the FinTech Law, a new figure was created, which is typically known as the Regulatory Sandbox. This figure is an attempt to open the way for and encourage innovation, investment and use of technological means for the provision of financial services in a different way from those existing in the market.

A Regulatory Sandbox, in terms of the FinTech Law, is defined as those that use technological tools or means, for the performance of a Reserved Activity, with modalities different from those existing in the market.

In this context, in order to operate a Regulatory Sandbox, prior authorisation must be obtained from the Financial Authorities or Banxico, depending on the type of activity to be carried out. Authorisation for the operation of a Regulatory Sandbox, in case it is granted, is temporary, so in no case may the authorisation be longer than three years.

The advantage of operating a Regulatory Sandbox is that it is possible to request exceptions to the legal provisions applicable to the regulated figures to allow a more efficient execution of a business model.

In order to include Financial Entities, the FinTech Law also contemplates the case in which these companies request authorisation to operate a Regulatory Sandbox in order to be able to offer a product or service without having to comply with all the applicable regulatory burden; that is, requesting exceptions or conditions to the application of the regulations. In this case, the authorisation, if granted, may not be longer than two years.

Under this figure, the entry of new competitors has been attempted as a result of the enthusiasm in the sector for the application and use of technology to speed up and facilitate the provision of financial services to the users of such services.

As of today, more than 10 applications have been submitted but have not been authorised by the corresponding Financial Authorities after more than five-and-a-half years since the Regulatory Sandbox was created. This has created an entry barrier for new competitors who no longer see a possibility in this figure for the implementation of their business models, but rather a disincentive in view of the negative resolutions issued by the Financial Authorities in the corresponding procedures.

It is important to note that we recently held the second edition of the Sandbox Challenge, the first contest of entrepreneurship and financial innovation that encourages world-class entrepreneurs to test their business models in the Mexican financial system.

The Sandbox Challenge was organised by the British Embassy and executed by Dai Mexico under the umbrella of the Financial Services Programme, where Legal Paradox® acted as a sponsor alongside giants such as Google, MassChallenge, ALLVP, among others. Among the more than 400 people who downloaded the competition rules for the Sandbox Challenge, the use of blockchain technology was the favourite means of innovation, followed by artificial intelligence.

For more information, please refer to Valderrama, Carlos, 2020, "*Regulatory Sandbox: The cornerstone for the fintech disruptive innovation's explosion in Mexico*", at FinTech Law, context, content and implications, Mexico City, Mexico, Tirant lo Blanch.

Ownership and licensing requirements

Non-Financial Entities that offer or facilitate to their clients the execution of Transactions with Virtual Assets are subject to compliance with the Anti-Money Laundering Legal Framework, which, as indicated above, includes the corresponding registration with the TAS and enrolment in the Internet Portal.

It should be noted that activities related to the analysis and issuance of investment recommendations on an individualised basis, as well as the obtaining of resources from the general public derived from the placement of shares for the regular and professional acquisition and sale of investment assets, are Reserved Activities in favour of Investment Advisors and Investment Funds, correspondingly. Therefore, if a company that offers or facilitates Transactions with Virtual Assets wishes to carry out these activities, it must also comply with the applicable financial regulations.

In terms of the SML, in order to carry out Reserved Activities for an Investment Advisor, it is necessary to obtain prior registration with the NBSC. In order to carry out Reserved Activities for an Investment Fund, in accordance with the Investment Funds Law, it is necessary to obtain prior authorisation also from the NBSC.

Mining

There are no specific regulations applicable to mining. However, in Mexico, there is a general principle: everything that is not prohibited by law is permitted for individuals or companies that do not carry out a Reserved Activity. Therefore, since there are no regulations or prohibitions applicable to mining, it is a permitted activity.

Notwithstanding the foregoing, mining has an important energy aspect in the proof-of-work protocols and, depending on the amount of energy required, a mining entity may be considered a "qualified user" that must comply with the required consumption or demand levels established by the Ministry of Energy under the Electricity Industry Law and is therefore subject to the corresponding energy legal framework.

Border restrictions and declaration

In Mexico, there are no specific rules applicable to border restrictions or obligations to declare the holding of cryptocurrencies, except for the existence of income derived from the sale of Virtual Assets (for further information, see "Taxation" above). However, it is important to mention that, from a tax perspective, our system is based on tax self-determination.

Regarding notices to be filed in relation to Transactions with Virtual Assets, see "Reporting requirements" below.

Reporting requirements

In the event that Banxico had determined or would determine in the future the possibility for Banks or FTIs to enter into Transactions with Virtual Assets with their clients, the Anti-Money Laundering Legal Framework would not be applicable to them, but rather the general provisions specifically applicable to each of them in matters of prevention of money laundering and financing of terrorism, which are issued by the MFPC.

The general provisions applicable to Banks provide the obligation to send quarterly reports to the FIU, through the NBSC, regarding Virtual Asset purchase transactions carried out regardless of the amount of the transaction, and a report for each Virtual Asset sale transaction carried out for an amount equal to or greater than the equivalent of US$2,250.

The general provisions applicable to FTIs also provide the obligation to send quarterly reports to the FIU, through the NBSC, in relation to Virtual Asset purchase transactions carried out regardless of the amount of the transaction; however, with respect to Virtual Asset sale transactions, a report must be sent when an individual transaction has been carried out for an amount equal to or greater than the equivalent of 7,500 investment units (as of today, approximately US$3,417).

Now, as previously mentioned, Non-Financial Entities are regulated by the Anti-Money Laundering Legal Framework when offering or facilitating to their clients the execution of Transactions with Virtual Assets. These entities must file monthly notices before the FIU through the Internet Portal containing, if applicable, information of clients who, within one month or in the accumulated of the last six months, have carried out purchase or sale operations of Virtual Assets for more than the equivalent of 645 measurement and updating units (as of today, approximately US$3,904.14). Also, these types of entities must submit, if applicable, the 24-hour notices referred to in points 8 and 9 of "Money transmission laws and anti-money laundering requirements" above.

It is curious that the regulation is currently designed to issue the corresponding reports/notices only in purchase and sale operations; that is, at times when there is a conversion

from fiat to Virtual Asset or *vice versa*, as if the transfer of the asset from one wallet to another would not generate any value or would not be subject to additional supervision, notwithstanding the international transfers that can be made with them.

Estate planning and testamentary succession

As for the inheritance of Virtual Assets, there is no specific regulation as of today, so the rules that apply are those of the common legislation on this matter.

It is worth mentioning that, in accordance with the regulation applicable to Non-Financial Entities that carry out Transactions with Virtual Assets, it is not mandatory to obtain from the client the data of a beneficiary to whom the assets existing in the corresponding account will be transferred in case of death.

Carlos Valderrama
Tel: +52 554 166 9048 / Email: carlos@legalparadox.com

Carlos is the founder and managing partner of Legal Paradox® with an LL.M., *summa cum laude*, and more than 18 years of experience, including expertise in lobbying FinTech and Blockchain Laws in Latin America.

Throughout his professional practice, Carlos has advised more than 380 Blockchain & FinTech projects of start-ups, scale-ups, unicorns and even traditional financial institutions. He has been part of the Central Bank Digital Currency Working Group led by R3, part of the international advisory board of the British Blockchain Association, and acted as FinTech Regulatory Advisor to the Financial Services Programme of the British Embassy in Mexico.

Carlos chairs the legal working group of global alliance LACChain for Mexico, an initiative of the Inter-American Development Bank to promote the use of Blockchain in Latin America and the Caribbean, and represents Mexico at the Blockchain Associations Forum.

Carlos is a professor of the subject in different universities in Latin America and trains members of the Bank of Mexico and other financial regulators in Latin America. He has been recognised as part of the top 2% of the world's best lawyers and named as one of the most disruptive digital lawyers in Mexico.

Arturo Salvador Alvarado Betancourt
Tel: +52 554 166 9048 / Email: arturo@legalparadox.com

Arturo graduated in 2021 with a Bachelor's degree in Law and in 2023 with a LL.M. in Financial Law Institutions, both degrees obtained from Universidad Panamericana.

His professional practice has focused on regulatory proceedings before Mexican financial authorities, prevention of money laundering, audits, drafting and negotiation of legal contracts, corporate law, protection of personal data, intellectual property, notarial law, and commercial and administrative litigation.

Previously, Arturo worked in the legal and compliance area at Cuenca, one of the first entities to be authorised in Mexico to operate as an Electronic Payment Funds Institution. He has certifications on AML matters issued by the National Banking and Securities Commission and the Mexican Financial Intelligence Unit. Furthermore, he has participated in the drafting of internationally published articles and has shared his experience within the FinTech sector at prestigious universities in Mexico and abroad.

Arturo is currently a senior associate at Legal Paradox®, the only boutique firm in Mexico focused on FinTech and Blockchain.

Legal Paradox®

Volcán 150 piso 4, Lomas de Chapultepec, CDMX, Mexico
Tel: +52 554 166 9048 / URL: www.legalparadox.com

Netherlands

Ilham Ezzamouri & Robbert Santifort
Eversheds Sutherland

Government attitude and definition

Government attitude

The Dutch Minister of Finance

In 2018, the Dutch Minister of Finance wrote a letter to the House of Representatives stating that the current supervisory and regulatory framework regarding cryptocurrencies[1] was inadequate. In view of the transnational nature of the market, a European or international approach was necessary. In addition, the Netherlands expressed its wish to play a pioneering role in the European Union with regard to the laws and regulations for cryptocurrencies in order to prevent any improper use, especially with regard to the inherent risks involved and the popularity of cryptocurrencies among criminals and terrorists.[2]

In 2020, the Dutch Minister of Finance again emphasised in a letter to the House of Representatives that European or international coordination of the regulation of cryptocurrencies would be preferable. Regulation would reduce the risks of money laundering and the financing of terrorism, but should also include rules on consumer protection, market integrity and capital requirements. The aim was – and still is – to set up a separate European regulatory framework for cryptocurrencies, which are not covered by existing laws and regulations.[3]

The Netherlands Bureau for Economic Policy Analysis

The Netherlands Bureau for Economic Policy Analysis (*Centraal Planbureau*, "**CPB**") is the Dutch government's main economic advisor. Recently, the director of the CPB stated that cryptocurrencies should be banned in the Netherlands, reasoning that a crash would be inevitable. Regulating cryptocurrencies would be counterproductive, because it legitimises cryptocurrencies as a financial product, which is the reason why – in his opinion – a total ban on the production, trade and possession of cryptocurrency should be put in place.[4] However, in June 2021, the Dutch Minister of Finance stated that regulation and supervision are more effective than banning cryptocurrencies outright.[5]

The Dutch Central Bank

The Dutch Central Bank (*De Nederlandsche Bank*, "**DNB**") has repeatedly warned about the risks of cryptocurrencies in recent years.[6] DNB has stated that cryptocurrencies are subject to volatile price swings, are susceptible to criminal abuse, and offer no consumer protection. At present, the regulation of cryptocurrencies focuses solely on anti-money laundering and countering the financing of terrorism ("**AML/CFT**"). Furthermore, DNB reports that it does not recognise cryptocurrencies as legal tender and that due to high volatility, cryptocurrencies are not suitable as a means of exchange. Currently, only fiat currencies, such as the Euro, are recognised as legal tender.[7]

In a report published in November 2022, DNB stated that uncovered cryptocurrencies are not suitable for serving as a reliable medium of exchange, store of value, or unit of account due to their highly volatile nature. DNB highlights the main issue as the lack of underlying assets for these cryptocurrencies, which poses challenges in evaluating their true worth. Moreover, a considerable portion of the supply is withdrawn from circulation by investors and developers, leading to increased price volatility caused by shifts in demand. The considerable price fluctuations and extensive attention on social media contribute to psychological effects, such as the "Fear of Missing Out" ("**FOMO**"), making it difficult for investors to disengage from the cryptocurrency phenomenon.

While uncovered cryptocurrencies possess an appealing aspect as speculative investments due to their volatility, this very characteristic hinders their ability to function effectively as a stable currency. Developed economies rarely adopt uncovered cryptocurrencies as a means of exchange because of their extreme instability, which makes them unsuitable for everyday transactions, especially considering the availability of national and European instant payment infrastructures. Additionally, the absence of a monetary authority to stabilise cryptocurrency values and the lack of prudential regulation or deposit guarantee schemes further contribute to the risks associated with these assets. According to DNB, prospective buyers must exercise great caution and be fully aware of the potential hazards before entering these markets, while regulatory authorities should be equipped with appropriate measures to monitor and mitigate the risks associated with market behaviour.[8]

As per the DNB report, uncovered crypto-assets are identified as unregulated securities. Promising new coins, based on novel distributed ledger technology ("**DLT**") networks, are typically developed by established companies (e.g., Ripple, BNB Chain, Algorand) or foundations (e.g., Ethereum, Solana, Avalanche), which may later transform into Decentralised Autonomous Organisations ("**DAOs**"). Developers are then either hired or secure funding by partnering with venture capital providers and conducting Initial Coin Offerings ("**ICOs**").[9] An ICO is comparable to an Initial Public Offering ("**IPO**"), wherein the issued crypto-assets could be viewed as company equity. However, in numerous instances, holders lack ownership, governance, or profit rights within the organisation, leading to limited legal protection and a lack of control.[10] Only about 3% of ICOs have such rights attached, potentially classifying them as securities.[11] Ultimately, it is probable that only a small fraction of uncovered crypto-assets fall within the purview of securities regulation.[12]

The value of uncovered crypto-assets, treated as securities, is determined by market supply and demand. Unlike traditional securities, these crypto-assets lack underlying assets or associated rights. Their pricing often depends on the likelihood of building a user network through the offered blockchain services. Holders of uncovered crypto-assets have no shareholder or creditor rights, and in case of a loss of trust, there are no assets that can be accessed. As a result, DNB emphasises that the value of these crypto-assets as securities remains uncertain and subject to volatility. Considering them as speculative investments, crypto-assets pose significant risks for consumer and investor protection, as highlighted by DNB. There is a potential for the cryptocurrency markets to become a threat to global financial stability due to their scale, structural vulnerabilities, and growing interconnection with the traditional financial system.[13] While the International Monetary Fund ("**IMF**") currently suggests that the cryptocurrency markets do not present a systemic risk, this assessment could change with further growth and integration into the traditional financial system.[14] Consequently, it is crucial to closely monitor these risks, particularly considering their global implications and the insufficient operational and regulatory frameworks in many jurisdictions. Additionally, the expansion of decentralised finance draws parallels

to the growth of shadow banking before the global financial crisis. The Financial Stability Board ("**FSB**") identifies four potential transmission channels between crypto-assets, the broader financial system, and the real economy: (1) exposures of the financial sector; (2) wealth effects for crypto holders; (3) confidence effects; and (4) the use of crypto-assets in payment and settlement systems.[15]

In conclusion, DNB's primary finding is that cryptocurrencies cannot be deemed equivalent to money.

In this report, DNB also highlights the potential in tokenising financial assets. By converting traditional financial assets into tokens on the blockchain, a secure proof of ownership is established. These tokens facilitate a quick and effortless transfer of financial assets, including the associated ownership and usage rights. Assets such as securities and real estate can be tokenised, eliminating the need for involvement from financial institutions during the transfer process.

DNB expresses a notable enthusiasm for stablecoins. Designed to address key drawbacks of uncovered cryptocurrencies, stablecoins offer a stable value and share the same unit of account as fiat currency, making them more suitable as a medium of exchange. This, in turn, could enhance the efficiency of cross-border payments and the settlement of tokenised assets. Furthermore, the potential for developing future applications related to Web3 is promising. However, it is essential to recognise that stablecoins also carry significant risks for monetary policy, given their operation outside the established monetary framework, as well as risks to financial stability due to their ties to the real economy, vulnerability to panic selling, and transaction settlement risks. Ensuring transparency, appropriate composition, and redeemability of the backing assets are key concerns, as issuers may be motivated to dilute assets or restrict redeemability. Hence, regulation is necessary to mitigate these risks.

While stablecoins may offer more stable pricing compared to uncovered cryptocurrencies, they bring another risk due to their direct link with the broader financial system. A lack of trust could trigger a run on stablecoins, potentially having significant consequences for the entire monetary system. There is also the inherent risk that stablecoin issuers might be inclined to increase returns on their assets once their stablecoins gain trust and usage. This could lead to the adoption of riskier assets or loans, reduce backing, or limit redeemability altogether. If the public becomes aware of inadequate asset backing, a bank run scenario could emerge. Therefore, the widespread unregulated use of stablecoins poses risks to the proper functioning of financial market infrastructures.

On an international level, DNB is committed to actively contributing to the development of international standards through collaboration with organisations such as the FSB, the Basel Committee on Banking Supervision ("**BCBS**"), and the Committee on Payments and Market Infrastructures ("**CPMI**"). Changes in European and national regulations, including the EU Markets in Crypto-Assets Regulation ("**MiCAR**") (in close cooperation with the Dutch Authority for the Financial Markets (*Autoriteit Financiële Markten*, "**AFM**")), and laws governing DNB's integrity oversight will shape DNB's responsibilities in the coming years. Additionally, international standards will continue to evolve, such as proposed revisions to capital requirements for banks regarding their exposures to crypto-assets, and the establishment of international standards for the transfer function of systemically important stablecoin arrangements.

In summary, DNB is well prepared to consistently monitor crypto-asset ecosystems, actively contribute to shaping regulatory frameworks, and adjust its supervision accordingly.[16]

Apart from the warnings and caution towards (services around) cryptocurrencies, DNB has a positive attitude towards introducing Central Bank Digital Currencies. DNB completed the initial exploratory phase, where it, among other things, conducted technical experiments with other central banks in the Eurozone. DNB will explore exactly what a digital Euro should look like. After that, a decision will be made as to whether the digital Euro will be realised.

The Dutch Authority for the Financial Markets

Like DNB, AFM does not recognise cryptocurrencies as legal tender. And like DNB, AFM repeatedly warns consumers especially about the risks of cryptocurrencies. AFM has warned investors, more specifically, about risks regarding ICOs.[17] Investing in ICOs does not differ in nature from participating in customary investment funds or IPOs. An important distinction is that ICOs are usually structured in a way that the cryptocurrencies are not subject to supervision by national regulators, such as AFM. AFM has stated that participating in ICOs is therefore not without risk and is comparable to joining an investment object (*beleggingsobject*) provider that does not require a licence for its services from a regulator.[18]

Following an investigation in December 2018, DNB and AFM prepared a number of recommendations for the Dutch government regarding cryptocurrencies. The first recommendation was to establish a Money Laundering and Terrorism Financing (Prevention) Act (*Wet ter voorkoming van witwassen en financieren van terrorisme*) licensing regime to tackle money laundering and terrorism financing in the exchange and storage of cryptocurrencies. The second recommendation was to adjust the (European) regulatory framework for corporate finance. DNB managed to realise the first recommendation, bringing into view the Fifth Anti-Money Laundering Directive (implemented as the Dutch Money Laundering and Terrorism Financing (Prevention) Act, "**Dutch AML Act**") (see the "Money transmission laws and anti-money laundering requirements" section below).

On 12 May 2022, the Head of Capital Markets Supervision and Transparency at AFM, Paul-Willem van Gerwen, shared his views on crypto-derivatives trading at the Amsterdam Propriety Traders Managers Meeting. According to Mr van Gerwen, AFM is of the opinion that trading in crypto-derivatives involves risks and that this market can be considered less mature than other derivatives markets. The volatility of crypto products in particular raises the question of whether the parties to the derivatives transaction will be able to keep their promises. Therefore, AFM is of the opinion that transactions with crypto-derivatives should be restricted to wholesale. According to Mr van Gerwen, crypto and derivatives are not (yet) suitable as means of payment and/or investment.[19]

As speculative investments, crypto-assets carry significant risks concerning the protection of consumers, investors, and the smooth operation of markets. Regulatory bodies responsible for consumer safeguarding and market behaviour, such as AFM in the Netherlands, frequently issue warnings about potential partial or total loss of invested funds. The primary risks faced by investors in crypto markets include: market illiquidity, making it challenging to sell crypto-assets; price volatility; and counterparty risks associated with crypto brokers, trading platforms, providers of crypto wallets for 19 cryptocurrencies, and other intermediaries. Additionally, there are risks concerning market integrity, encompassing fraud, theft, and market manipulation, as crypto markets and infrastructures may not function fairly and securely. Information regarding risks could be incomplete, inaccurate, or unclear, potentially disadvantaging certain investors compared to others, especially private investors, who are also at risk due to crypto trading platforms often directly offering crypto-assets to consumers. Admission procedures may be insufficient in preventing illegal and fraudulent sellers and in safeguarding investors with limited knowledge or an inappropriate risk profile.[20]

Definitions

Various definitions are used when referring to cryptocurrencies. AFM and DNB have chosen to use the more neutral term "cryptos", since the phenomenon is still in development, takes on many forms and currently does not function in the same way as fiat currency.[21] The definition that AFM and DNB use matches that of the definition in the Dutch AML Act of "virtual currency", which is currently the only official definition of cryptocurrencies in European legislation:

> "*A digital representation of value that is not issued or guaranteed by a central bank or a public authority, is not necessarily attached to a legally established currency and does not possess a legal status of currency or money, but is accepted by natural or legal persons as a means of exchange and which can be transferred, stored and traded electronically*."[22]

In addition, AFM and DNB have adopted a taxonomy that is frequently used on an international level, which distinguishes between three overlapping categories of cryptocurrencies: transaction crypto(s); utility crypto(s); and investment crypto(s).[23] These categories are highly interconnected, as these "cryptos" can have multiple functions simultaneously, and their function may change over time. For example, an investment crypto may transform over time into an utility crypto or a payment crypto.[24]

1. **Transaction crypto(s)**
   Transaction cryptos are cryptocurrencies that are meant to be used for general transactions or value transfers. However, AFM and DNB stated that this does not imply that they are an alternative to existing fiat currencies. Users can effect global peer-to-peer transactions without the involvement of a third party (such as a bank). Bitcoin and Litecoin are the best-known examples of transaction cryptos.
2. **Utility crypto(s)**
   Utility cryptos are cryptocurrencies that give the owners a right to the use of (or access to) a specific application/service offered by or through a provider's platform (blockchain-based or otherwise). Well-known examples are Ether, which gives users the right to use or access services running on the underlying Ethereum network, and Filecoin, which enables users to purchase decentralised cloud storage.
3. **Investment crypto(s)**
   Investment cryptos are cryptocurrencies that are being used as an alternative for, or in addition to, existing financial instruments such as cash-traded products such as stocks, bonds, and currencies. AFM and DNB have stated that some investment cryptos may qualify as financial instruments as defined in the Financial Supervision Act (*Wet op het financieel toezicht*, "**FSA**"), while other investment cryptos are structured in a way that prevents them from qualifying as such.[25] These investment cryptos therefore fall outside the scope of the FSA.

Cryptocurrency regulation

In general

In the Netherlands, the FSA, the Dutch AML Act and the Prospectus Regulation are the most relevant rules and regulations of the regulatory framework for cryptocurrencies, cryptocurrency services and cryptocurrency providers. In the FSA, European directives such as the Markets in Financial Instruments Directive 2014/65/EU ("**MiFID II**") and the Alternative Investment Fund Managers Directive 2011/61/EU ("**AIFMD**") are implemented. Apart from the Dutch AML Act (see the "Money transmission laws and anti-money laundering requirements" section below), these rules and regulations do not contain

provisions that are specifically tailored to cryptocurrencies. Cryptocurrencies and related activities are subject to the existing regulatory framework as far as possible.

The FSA does not hold a definition of cryptocurrencies (or any digital asset). It depends on the characteristics of the cryptocurrency whether it falls within the scope of the FSA. In cases where the FSA is indeed applicable, the cryptocurrency most often qualifies as (i) a financial instrument, more particularly a security, (ii) a participation right in an alternative investment fund (*alternatieve beleggingsinstelling*, "**AIF**"), or (iii) in some cases, an investment object.

According to Article 1:1 FSA, a security[26] is (i) a negotiable share or an equivalent right, (ii) a negotiable bond or other negotiable debt instrument, or (iii) any other negotiable instrument issued by a legal person, company or institution by which securities referred to under (i) or (ii) may be acquired through exercising the rights attached to this instrument, or that can be settled in cash. AFM provided some practical guidance on when tokens may qualify as securities within the meaning of the FSA by, among other things, explaining the term "negotiability" and emphasising that, for qualification as security, the rights linked to a token are the decisive factor. In general, AFM decides on a case-by-case basis whether a security token constitutes a security. If a token qualifies as a security, the issuing entity and/or possible other entities involved are subject to the Prospectus Regulation and requirements of MiFID II as implemented in the FSA.

Another possibility is that a token qualifies as a participation right in an AIF. The rules for AIFs are laid down in the AIFMD. The AIFMD is implemented in the FSA. According to Article 1:1 FSA, an AIF is defined as a collective investment undertaking (including investment compartments of such an undertaking) that raises capital from a number of investors, with the purpose to invest in accordance with a defined investment policy for the benefit of those investors. It is prohibited to manage an AIF or to offer units in an AIF in the Netherlands without a licence from AFM, unless an exception and/or exemption is applicable.

In some cases, a cryptocurrency may qualify as an investment object within the meaning of the FSA. It is prohibited to offer an investment object in the Netherlands without a licence obtained from AFM. The Dutch regulatory regime for investment objects is local regulation. In the FSA, an investment object is defined as "an object, a right to an object or a right to the full or complete return in cash or part of the proceeds of an object, […] which is acquired for payment at which acquisition the acquirer is promised a return in cash and where the management of the object is mainly carried out by someone other than the acquirer". The regulatory regime for offerors of investment objects is very strict.

Please note that cryptocurrencies do not qualify as money (*geldmiddelen*) within the meaning of the FSA. Under the FSA, money is defined as cash (*chartaal geld*), scriptural money (*giraal geld*) and electronic money (*elektronisch geld*). Cash is not defined in the FSA but refers to money in the physical form, such as banknotes and coins. Scriptural money is also not defined in the FSA, but can be described as a claim that account holders have on their bank due to a positive balance on their bank account. The FSA does have a definition of electronic money, however. According to the FSA, electronic money is – in short – electronically, including magnetically, stored monetary value as represented by a claim on the issuer that is issued on receipt of funds for the purpose of making payment transactions, and which is accepted by a natural or legal person other than the electronic money issuer. This definition has been derived from the E-Money Directive 2009/110/EC. Most cryptocurrencies are not issued by a central body but are decentralised. Cryptocurrencies therefore do not represent a claim on the issuer and are not necessarily

issued in exchange for traditional money. This means that under the FSA, cryptocurrencies do not qualify as electronic money. If a cryptocurrency does qualify as electronic money because it has an issuer and meets the other requirements of the definition, it is prohibited to issue said electronic money without a licence from DNB.

The position of AFM and DNB is that the regulation (trade) of cryptocurrencies should be regulated at international level in order to be effective. Therefore, prior to MiCAR becoming effective in 2024, there are no national laws or regulations that specifically address crypto-assets.

On 30 June 2022, the Council presidency and the European Parliament reached a provisional agreement on the European Commission's MiCAR proposal.[27] The purpose of MiCAR is to protect customers against some (i.e., not all!) of the risks associated with investment in crypto-assets. MiCAR is applicable to crypto-assets and crypto services that do not fall under any other European regulatory regime (for example, MiFID II).

Crypto-asset issuers that fall within the scope of MiCAR will be required to first publish a whitepaper, which must contain core information on the characteristics, rights and obligations, and underlying technology and project – a sort of prospectus-light information document.

In addition, crypto-asset service providers ("**CASPs**"), which include trading platforms and exchange providers of crypto wallets, will need an authorisation to operate within the European Union and, in order to obtain such authorisation, will need to have specific governance arrangements and risk management in place. Persons who provide custody and administration of crypto-asset services will also be liable to clients for losses of crypto-assets resulting from "malfunction or hacks" up to the market value of the crypto-asset lost.

Stablecoins, which have lately been the subject of discussion and scrutiny, are also specifically targeted. Large stablecoin issuers will have to maintain reserves to cover all claims and provide immediate redemption to holders.

MiCAR also includes market abuse regulation – similar to but a lighter version of the MAR – to prohibit fraudulent behaviour (insider dealing, market manipulation). The implementation of MiCAR necessitates national legislation, which is currently undergoing consultation in the Netherlands. The consultation aims to enforce the Regulation on information accompanying transfers of funds and transfers of certain crypto-assets, which also introduces amendments to the Fourth Anti-Money Laundering Directive. The proposed bill mainly focuses on modifications to the Dutch AML Act due to the amendment of the Fourth Anti-Money Laundering Directive. The most significant change to the Dutch AML Act involves extending its scope to cover CASPs falling under MiCAR. The bill designates AFM as the supervisor for CASPs, rendering the current registration regime for crypto parties obsolete.

Almost a year later, on 9 June 2023, the Regulation was published in the Official Journal of the European Union. The rules will enter into force in phases, with most provisions applying from 30 December 2024.

MiCAR does not encompass all aspects of DLT. There are significant exceptions, including that crypto-assets that qualify as financial instruments under MiFID II are not covered by MiCAR. They remain subject to the financial regulations outlined in MiFID II. Non-fungible tokens ("**NFTs**"), which are unique and not interchangeable with other crypto-assets, are outside the scope of MiCAR. However, within 18 months, the European Commission will be mandated to conduct an assessment and, if necessary, propose new regulations for NFTs.

The main changes under MiCAR include a specific focus on stablecoins, which will be subject to strict conditions and supervision. Issuers of stablecoins will need to maintain sufficient liquid reserves and minimum liquidity to provide consumers with greater protection. It is

important to note that technical standards and delegated acts specifying certain elements of MiCAR will need to be adopted before the Regulation becomes applicable. MiCAR will impact crypto-assets currently outside European and national regulations, encompassing "payment tokens" and "utility tokens", and will have implications for crypto-asset issuers and service providers within the European Union.

Licensing instead of registration

Currently, crypto service providers are required to adhere to a registration regime under the Dutch AML Act. However, with the introduction of MiCAR, parties will be obliged to obtain a licence to operate as crypto service providers.

Although MiCAR imposes stricter requirements than the current registration regime under the Dutch AML Act, the implementation of the Regulation also brings certain advantages. For instance, a permit obtained under MiCAR can be "passported" to other EU Member States, a possibility not available under the current registration regime. This presents an opportunity for Dutch crypto service providers to access a broader market within the European Union.

MiCAR and AML/the Dutch AML Act

The existing AML legislation partially applies to certain crypto service providers, such as providers of exchange services and custodian wallets. Nevertheless, MiCAR includes additional AML measures:

- The European Banking Authority ("**EBA**") will establish and maintain a public register of non-compliant crypto service providers.
- Crypto service providers that have their parent companies established in countries considered high risk for money laundering according to an EU list, or listed on the European Union's non-cooperative jurisdictions for tax purposes, will be subject to more stringent AML checks.

Stricter requirements will also apply to shareholders and directors of crypto service providers, especially regarding their location.

Environmental, social, and governance

The crypto-asset market will be required to disclose information about its environmental and climate impact. The details on how this will be carried out will be further outlined by the European Securities and Markets Authority ("**ESMA**"). Notably, the decision was made to not ban crypto-assets utilising the "Proof of Work" algorithm, despite their high energy consumption.

As of 30 December 2024, crypto service providers will need a licence to continue their operations as crypto service providers. Otherwise, they will likely have to suspend their business activities until the permit is obtained.[28]

The legislation will undoubtedly have a significant impact on consumers. The focus of MiCAR lies on crypto-assets and CASPs. The latter encompasses companies offering services related to crypto-assets, such as crypto exchanges, wallets, and lenders. Under MiCAR, CASPs must adhere to stringent rules to ensure enhanced consumer protection and foster greater trust within the crypto sector. These rules include meeting minimum capital requirements, segregating client assets from company ownership, providing efficient complaint-handling procedures, and offering comprehensive information about the associated risks. Additionally, service providers must actively prevent market manipulation. The need for these rules becomes apparent when considering past incidents involving CASPs in scandals. The *Mt. Gox* case in 2014, where approximately 740,000 Bitcoins were stolen, and the recent bankruptcy of FTX due to a weak balance sheet and missing client assets, underscore the necessity for robust consumer protection measures.

Increased trust and transparency in the crypto sector

More stringent regulation can contribute to bolstering trust within the crypto sector. Companies operating within this space are subjected to increased rule compliance and rigorous monitoring. For instance, MiCAR requires a digital currency to submit a whitepaper to the regulator before being permitted on the European market. These whitepapers contain comprehensive details about the cryptocurrency, its functionality, and the associated risks, thereby promoting greater transparency.

Power of regulators[29]

With MiCAR, national regulators are granted extensive powers. They have the right to request information at any time and can demand that the whitepaper be amended if they believe essential information is missing. In case of non-compliance with the law, they can prohibit the provision of services and have the authority to publicly disclose them in violation of the law. Additionally, the regulators are equipped with intervention measures that allow them to temporarily halt the sale of certain cryptocurrencies or the provision of specific services.

A more stable future for stablecoins

The crypto sector faced upheaval in May 2022 when the ecosystem of Terra (LUNA) and its associated TerraUSD (UST) collapsed, leading to a loss of value in the UST stablecoin due to a fall in LUNA's market value. The incident prompted regulators to focus on stablecoins, leading MiCAR to address them extensively. The rules pertaining to stablecoins aim to ensure their stability and coverage, allowing investors to exit without losing value. By setting these guidelines, MiCAR expects to instil greater stability and reliability in consumer-oriented stablecoins.

Distinguishing between reliable and unreliable players

MiCAR brings more transparency to the crypto market by distinguishing between reliable and unreliable players. Regulated and compliant companies are deemed reliable, aiding consumers in making better-informed decisions when selecting a crypto service provider.[30]

Token sale (ICOs)

In the Netherlands, there are no special rules and regulations for ICOs. An ICO and the regulatory requirements that may come with it will be based on the existing legal framework for the provision of traditional financial services, i.e., FSA and relevant European regulation.

General Data Protection Regulation

The Dutch Data Protection Authority (*Autoriteit Persoonsgegevens*) has announced that it will closely monitor the area of cryptocurrency, including developments, for the period 2020–2023. Even though the Authority has stated that it will focus on "data protection in a digital society", including the internet of things and artificial intelligence, it has not addressed the use of blockchain and/or the processing and deletion of personal data on the blockchain. Currently, no guidance on the use of blockchain in relation to the General Data Protection Regulation has been issued by the Dutch Data Protection Authority.

Financial regulatory laws and NFTs

Under the current regulatory framework in the Netherlands, NFTs themselves remain unregulated. However, NFTs or NFT-related services may potentially fall within the scope of other regulated products and/or services:

- Regulated products: Depending on its characteristics, an NFT could be considered (i) a security (*effect*), (ii) an investment object (*beleggingsobject*), (iii) a derivative (*derivaat*), (iv) e-money (*elektronisch geld*), or (v) an art object (*kunstvoorwerp*).

- Regulated services: Under certain circumstances, NFT-related services might also be subject to regulation; for instance, if one plays a role in the payment or exchange process related to the buying and selling of NFTs, or if funds or NFTs belonging to clients are held.

NFTs exist in various forms, and despite their current lack of specific regulation in the Netherlands, it is possible that an NFT or NFT-related service could fall under the scope of other regulated products or services. Organisations intending to issue or offer NFTs, or provide services such as operating an NFT platform or NFT brokerage, should analyse whether their NFTs or services are subject to Dutch financial regulatory laws and, if so, which financial regulatory requirements would apply.

The term "crypto-asset" is broad and generally includes NFTs, except for crypto-assets that are "unique and not fungible with other crypto-assets". For an NFT to fall under this exception, both the NFT itself and the assets or rights it represents must be "unique and non-fungible". Fractional parts of a unique and non-fungible crypto-asset are not covered by the exception and are, therefore, generally within the scope of MiCAR. The determination of whether an NFT is unique and not fungible depends on its actual features and characteristics, rather than simply its classification as an NFT by the issuer. Regardless of whether they fall under MiCAR's scope, consideration should also be given to whether an NFT or NFT-related service might be subject to other legal frameworks.

Taxation

Income tax

The capital gains on digital assets, such as cryptocurrencies, realised by a private individual are subject to income tax in the Netherlands. Private individuals that own cryptocurrencies should declare their cryptocurrencies on their Dutch tax return form, based on the value of the cryptocurrency and the applicable exchange rate on 1 January of the concerned tax year (*the reference date*).[31]

There are no regulations (yet) for determining which cryptocurrency exchange rate should be applied. The State Secretary of Finance has stated that, in the absence of a statutory regulation, the exchange rate of the applicable exchange platform should be applied.[32] However, this approach does not take into account the fact that cryptocurrencies can also be stored in a so-called *offline wallet*, which is not connected to an exchange platform.[33] In such case, we would advise applying the exchange rate of the exchange platform that is used most frequently by the private individual.

In the Netherlands, income is taxed in three different categories with different taxation rates, also known as "Boxes". Assets are normally taxed in Box 3 (*income from assets*).[34] However, when an individual actively pursues the growth of his assets, these may also be taxed in Box 1 (*income from other activities*).[35] In that case, income from assets is regarded differently to normal asset management.[36] The exact determination criterion cannot be defined; it depends on a combination of knowledge and experience, time spent and tools purchased. Any combination of these three factors can, in theory, result in a shift of assets from Box 3 to Box 1. The taxation of assets in Box 3 is considerably lower than in Box 1. In Box 1, the actual return is taxed at a rate of up to 49.5%, while in Box 3, the fictitious return is taxed at a rate of 31%.[37]

In the following cases, the assets are transferred from Box 3 to Box 1:

- Is an individual's knowledge when trading in cryptocurrency no more than an educated guess of generally known circumstances? If the answer to this question is yes, the income will be taxed in Box 3.

- Does an individual have special (advanced) knowledge when trading so that the uncertain part of the transaction is eliminated? If the answer to this question is yes, the income will be taxed in Box 1.
- Is trading in cryptocurrency a daily activity? If the answer to this question is yes, the income will be taxed in Box 1.
- Has an individual purchased and used IT equipment to "mine" cryptocurrency? If the answer to this question is yes, the income will be taxed in Box 1. However, the value of the cryptocurrency itself will be taxed in Box 3.
- Does an individual manage the assets or IT equipment for others in return for payment? If the answer to this question is yes, the income will be taxed in Box 1.

When any of the above activities are carried out by an individual for his own company, the result of these activities will be taxed in Box 1 (*income from profits*).[38]

Corporate tax

The capital gains on digital assets such as cryptocurrencies realised by a company are subject to corporate tax in the Netherlands. The results of mining and trading of cryptocurrencies should therefore be expressed in the profit and loss account. The results must be taken into account in accordance with good business practice.[39]

If a company is paid in cryptocurrencies for its services or supplies, it must convert the cryptocurrencies into fiat currency (EUR). The converted amount should be included in the turnover. When converting the cryptocurrencies, the company can make a profit or loss (depending on the estimated value on the reference date). This is reflected in the profit and loss account. When a company owns cryptocurrencies on its balance sheet, the cryptocurrencies will be valued at cost price or the lower market value. In such case, the exchange rate of the exchange platform that is used (or from which the cryptocurrencies originate) will be applied.

Two taxable income brackets are applicable for corporate tax. A lower rate of 16.5% applies to the first income bracket, which consisted of taxable income up to €200,000 in 2020, and has increased to €245,000 in 2021. A standard rate of 25% applies to the excess of the taxable income.[40] The first bracket will be extended further in 2022 to a taxable income of up to €395,000.[41]

Value-added tax

The Court of Justice of the European Union has ruled that Bitcoin does not serve any purpose other than making payments, and that the "currency exemption" therefore applies. The Court of Justice of the European Union held that it is irrelevant whether a cryptocurrency, such as Bitcoin, is legal tender in a country or not, as Bitcoin is still, for value-added tax ("**VAT**") purposes, a currency.[42] Consequently, the purchase and sale of cryptocurrencies used as means of payment have been exempted from VAT. The purchase and sale of goods or services that are subject to VAT, and which are paid for in cryptocurrencies, are therefore treated no differently from payments with fiat currency.[43] Finally, mining as such is not subject to VAT, because the recipient of the mining services cannot be determined.[44]

Tax rules on NFTs

There is no definition of an "NFT" in EU legislation or Dutch domestic laws.

The recent EU working paper on NFTs acknowledges the necessity to determine the VAT treatment of NFTs based on the specific characteristics and purpose of the transactions. It defines an NFT as a digital unit (token) on a "distributed ledger", comprising an identification code and metadata. The identification code serves to identify the token, while the metadata pertains to what the NFT represents: the asset. This asset could encompass a digital portrait painting or the ticket to a physical concert, depending on the NFT.

Determining the appropriate tax treatment of NFTs can be challenging due to the lack of clear guidance, although certain instances may find clarity through generic Dutch tax rules. The Dutch tax implications, including complications and uncertainty, related to specific uses of NFTs are as follows:

- **Wage tax**: When an employee receives an NFT, it is generally considered a non-cash benefit, subject to regular Dutch wage withholding tax. Consequently, the Dutch employer must withhold the applicable Dutch wage withholding tax on the NFT's value and remit the tax in EUR to the Dutch tax authorities. Valuation issues may arise, as determining the NFT's value in EUR (as opposed to a cryptocurrency such as Bitcoin) might be difficult.
- **Gift tax**: Donations in the form of NFTs are treated no differently from regular cash or in-kind donations. Valuation implications may also arise concerning NFT donations, which should be valued at fair market value at the time of the donation.
- **Personal income tax**: The tax treatment of NFTs depends on whether an individual is a passive investor or engaged in business activities involving NFTs. A Dutch passive investor owning NFTs typically will not be subject to tax on income and capital gains realised on the NFTs. Instead, they are taxed at a flat rate of 32% (2023) on deemed income equal to 6.17% (2023) of the NFTs' value at the start of the calendar year. A Dutch individual conducting business activities with NFTs may be subject to tax on income and gains derived from the NFTs at progressive tax rates up to 49.50%. Determining whether activities such as minting, owning, or selling NFTs go beyond normal asset management and constitute conducting business activities requires the consideration of all relevant facts and circumstances.
- **Corporate income tax**: For corporate taxpayers, the tax consequences are relatively straightforward: any income derived from NFTs should generally be included in taxable income; and corporate costs related to minting or selling NFTs should typically be deductible or capitalised.
- **Real estate transfer tax**: It is likely that the Dutch real estate transfer tax ("**RETT**") will apply to the acquirer of an NFT representing 100% of the economic ownership of Dutch real estate. Existing Dutch RETT laws generally tax economic ownership transfers, regardless of the instrument used for the transfer. Clear guidance from the Dutch tax authorities could provide certainty and address the application of RETT exemptions as well.
- **VAT**: Based on the EU working paper on NFTs, each transaction linked to an NFT may be subject to different VAT treatment, depending on whether it is a supply of services or goods, whether consideration is involved, and whether the supply is made by a taxable person. The working paper on NFTs concludes that categorising NFTs solely as electronic services may not fully capture the complexity of the situation and urges caution in making hasty conclusions. Without precise categorisation of NFTs, taxpayers are left to interpret existing Dutch tax laws, which may not adequately cover the unique characteristics of an NFT. Explicit guidance from the Dutch tax authorities on NFTs would be beneficial.[45]

Money transmission laws and anti-money laundering requirements

Money transmission laws

There are currently no regulations that explicitly prohibit the use or trading of crypto-currencies in the Netherlands. However, cryptocurrencies that are used as means of payment to third parties may trigger certain regulatory requirements under the FSA in which the Payment Services Directive[46] is implemented.

AML/CFT requirements

On the basis of the Act implementing amendments to the Fourth Anti-Money Laundering Directive, implemented in the Dutch AML Act, crypto service providers, i.e., firms offering services for the exchange between virtual and regular currencies, and providers of custodian wallets for virtual currencies, must request registration with DNB.

The registration application is extensive and has many similarities to a licence application. In the explanatory notes to the form for registration as a crypto service provider from DNB,[47] the requirements for registration are described in detail. For registration, the crypto service provider needs to provide:

- Company details, such as a recent extract from the Trade Register of the Chamber of Commerce of the company, a certified copy of the company's articles of association, and a copy of the company's up-to-date shareholders' register.
- A business plan, including a schematic overview of the company's activities and strategy.
- Evidence of good governance, including an organisation chart, and a description of transparent control structure.
- Evidence of sound operational management, such as a description of the company's independent compliance function and audit function, a reporting procedure for Dutch AML Act incidents, a policy for outsourcing activities that are related to the Dutch AML Act and the Sanctions Act, copies of any outsourcing agreements that are relevant in the context of compliance with the Dutch AML Act and the Sanctions Act, and an education and training policy.
- Evidence of ethical operational management, including a systematic integrity risk analysis, an integrity policy, a customer due diligence policy, a description of the company's customer due diligence procedure, a sanctions screening policy, a description of the sanctions screening policy, and a policy for transactions monitoring and reporting of unusual transactions and a description thereof.

Furthermore, the crypto service provider must submit initial assessment forms through which each (co-)policymaker[48] will be subjected to a fit and proper screening by DNB, and initial assessment forms through which shareholders owning 10% or more of the shares in the entity (so-called "qualifying shareholders") are screened on propriety, including the ultimate beneficial owner reputation test (which applies as of 21 May 2021).

The registration procedure as determined by DNB caused a lot of discussion, not only in the crypto service providers market, but also in the legal world. The question arose whether DNB had the authority to shape this registration requirement based on the Fifth Anti-Money Laundering Directive as a disguised licence requirement. On 7 April 2020, the District Court of Rotterdam[49] considered (among other things) that it is doubtful whether DNB was authorised to work out the registration requirement of the Fifth Anti-Money Laundering Directive as it did in the Dutch AML Act. The Court also considered that the registration requirement has great similarities with a licence regime. Although this proceeding was a preliminary relief proceeding and the Court did not suspend the registration requirement for the claimant because it felt that more thorough investigation was needed, it did fuel the debate, which is ongoing. Another notable consideration in this judgment is that the Court questioned whether a crypto service provider is required to determine the identity of the sender or recipient of a transaction, to check whether this person is mentioned on the sanctions list, and to determine whether this person is indeed the sender or the recipient of the transaction. According to DNB, the crypto service provider needs to perform this action per transaction.

A registration obligation for crypto service providers was introduced on 21 May 2020 because crypto services often involve an increased risk of money laundering and terrorism financing. This is due to the anonymity associated with crypto transactions. If there were no obligation to register, it would not be possible to monitor whether the risk of criminal financial flows was sufficiently mitigated.

The Dutch AML Act aims to combat the laundering of criminal income and the financing of terrorism. It is vital that money laundering is combatted, in order to combat crime effectively. After all, concealing the criminal source of criminal proceeds enables the perpetrators of these crimes to remain out of reach of the investigative authorities and to enjoy the accumulated assets undisturbed.

By offering crypto services in the Netherlands without registration with DNB, Binance has frustrated the objectives of the Dutch AML Act. For example, Binance cannot report any unusual transactions to the Netherlands Financial Intelligence Unit. As a consequence, a large number of unusual transactions may remain out of sight of the investigative authorities.

On 25 April 2022, DNB imposed an administrative fine of €3,325,000 on Binance Holdings Ltd.[50] The amount of the administrative fine was determined on the basis of DNB's General Fines Policy. It was decided to increase the basic amount of the fine on the basis of increased seriousness and culpability.

In increasing the fine, DNB took into account that Binance is currently the largest provider of crypto services worldwide and that Binance has a very large number of customers in the Netherlands. It also took into account that Binance had a competitive advantage because it did not pay any fees to DNB and did not have to incur any other costs in connection with ongoing supervision by DNB. The breaches also took place over a long period of time, from 21 May 2020 (the date of introduction of the registration obligation) until at least 1 December 2021 (the date of completion of DNB's investigation). DNB therefore considers these violations to be very serious.

However, DNB has moderated the fine by 5%, because an application for registration has now been submitted and because Binance has been relatively transparent about its operations throughout the process. Meanwhile, Binance has ceased its operations in the Netherlands due to its alleged difficult regulatory environment.

Promotion and testing

Fintech support by the regulators

In order to further promote the use of blockchain and share knowledge regarding blockchain technology, governmental and regulatory bodies, universities, research organisations and (multi)national private entities have formed a coalition named the "Dutch Blockchain Coalition". Currently, the Dutch Blockchain Coalition is creating and facilitating an environment in which reliable blockchain applications can be developed and utilised in a secure manner.

Despite the regulators' focus on AML/CFT, DNB and AFM have also taken a more constructive and practical approach, as they have jointly established the "Innovation Hub" in order to offer businesses support on innovative financial products and services, such as cryptocurrencies.

Public support for innovation in the area of cryptocurrency

The Netherlands has a good starting position in the digital landscape, with a high degree of digitisation and a very good digital infrastructure. This makes the Netherlands an excellent

breeding ground for the emergence of novel innovations and growth of technological developments in the field of cryptocurrency and blockchain.

In recent years, both private parties and public-private partnerships have organised blockchain hackathons, including the Dutch Blockchain Hackathon, organised by the Dutch Blockchain Coalition, and the NEO Blockchain Hackathon, organised by blockchain-based smart economy platform NEO and the Delft University of Technology. These initiatives exemplify the willingness to innovate in the growing field of blockchain.

Ownership and licensing requirements

From a Dutch civil law perspective, there are two qualification questions. The first question is whether cryptocurrencies qualify as legal tender (*wettig betaalmiddel*). There is ample agreement in case law, literature and amongst the Dutch legislator and regulators that cryptocurrencies do not qualify as legal tender.[51]

The second question is how to qualify cryptocurrencies within the Dutch civil law system. Although it seems clear that cryptocurrencies do not qualify as tangible property, it is commonly assumed by legal literature and in case law that – by taking a practical approach while skipping the fundamental questions – cryptocurrencies qualify as (some sort of) property right (*vermogensrecht*).[52]

On 14 February 2018, the District Court of Amsterdam considered that Bitcoin has all the characteristics of a "property right, which means that Bitcoin represents a value and is transferable. According to the Court, a Bitcoin is a unique, digitally encrypted series of numbers and letters stored on the hard drive of the right-holder's computer. Bitcoin is "delivered" by being sent from one wallet to another as a payment. The Court ruled that a Bitcoin therefore represents a value and is transferable. The Court added that Bitcoin is a legitimate "transferable value".

There are several legal writers who have argued that the most correct qualification of cryptocurrency under Dutch civil law is to focus on the public key and to qualify the public key as a bill of exchange. The reasoning being that, like with a bill of exchange, the holder of the public key is ultimately the person who controls the cryptocurrency.[53]

The question of whether assets stored on the blockchain or that have been minted (such as NFTs) are susceptible for other proprietary rights, particularly copyrights, remains subject to debate. For example, one could argue that a majority of the "Bored Apes" NFT issues – despite applicable (licensing) terms – fail to comply with the criteria of originality or even creation by a human being.

In the Netherlands, it is also possible to levy a prejudgment or executory attachment on Bitcoin (and most likely similar cryptocurrencies). It is important to realise what to attach. First of all, the crypto wallet on which the cryptocurrencies are stored should not be equated with a bank account with a bank. Hence, the rules for attaching bank accounts do not apply. It is ultimately the owner of the crypto wallet that, through its public and private key, has access to the cryptocurrencies in the crypto wallet. Therefore, the attachment should be directly on the crypto wallet. However, attaching the computer or other device from which the owner manages its crypto wallet is obviously without any effect as the crypto wallet is accessible from each and every device through the cloud. Therefore, the bailiff should take effective control over the cryptocurrency by transferring the cryptocurrency to a crypto wallet held by the bailiff for that purpose. This requires the public key, which the owner of the crypto wallet should provide based on information obligations on the attached debtor following from Dutch Supreme Court case law.[54]

Mining

Currently, mining cryptocurrencies as such is permitted in the Netherlands and no specific permits are required. However, if the mining activities take place on a large scale, the mining hardware will require significant amounts of energy, and additional safety is needed. Furthermore, large-scale mining techniques will result in (additional) environmental emissions. Under such circumstances, permits, such as an environmental permit, may be required.

Furthermore, DNB takes a more active interest into the carbon footprint of Bitcoin. In 2021, DNB published its findings on the impact of cryptocurrencies on the climate in its paper "The carbon footprint of bitcoin".[55] This analysis shows that Bitcoin and Etherium use an energy-intensive algorithm. The findings are based on a new methodology to calculate the carbon footprint of Bitcoin. The results show that the climate impact per transaction equates to two-thirds of the monthly emissions of an average Dutch household, which is an increase of 32% compared to 2019.

For now, this is part of DNB's continuous effort to provide more insight into the climate impact of the financial sector, but this may turn into regulatory action at some point.

In a judgment published on 15 October 2021, the Dutch District Court of The Hague ruled that Bitcoin mining activities constitute an "economic activity" within the meaning of Article 9 of VAT Directive 2006/112. In order to fall within the scope of the VAT Directive, taxable parties must carry out such an "economic activity". In this case, the claimant was engaged in the verification and authentication of transactions in the cryptocurrency Bitcoin and the creation of blocks within the Bitcoin blockchain (mining activities). The blockchain served as a digital ledger in which all transactions in Bitcoin were logged. The creation of blocks created room for (new) transaction data. The claimant received two types of remuneration for these activities: transaction remunerations; and block remunerations. The fees consisted of payments in Bitcoin. The fees for all the above activities were allocated on a winner-takes-all basis: the first to realise a block received all the transaction fees for the block as well as the full block reward; the others received nothing.

At issue was whether the mining activities could be considered "economic activities". The Court held that the transaction fees could be seen as remuneration for the claimant's activities in validating the transaction. The fact that the claimant does not always receive a transaction fee does not alter this.

In addition, the Court considered that the validation of transactions is so closely related to the creation of blocks on the blockchain that they are inextricably linked. Both activities are aimed at receiving the remuneration, as a validated transaction can only be verified when it is created on the blockchain. Therefore, the Court considers that validation, verification and coin mining are inseparably intertwined, all of which are mining activities that should be seen as a preparatory "economic activity" indispensable to Bitcoin trading.

As the mining activities qualify as an economic activity, they are exempt from VAT on the basis of Article 135(1)(d) of the VAT Directive. This may be an interesting precedent for the mining of other cryptocurrencies, but may also be relevant for the VAT treatment of the cessation of cryptocurrencies.

The next question of this case was whether the claimant, based on statistical data showing that 98% of Bitcoin trade is in fiat currencies other than the currencies of EU Member States, proved that its customers were located outside the European Union, which would entitle it to a VAT reduction under Article 169(c) of the VAT Directive.[56] According to the Court,

the currency in which Bitcoin is traded is not sufficient to conclude that the customers are established outside the European Union, as customers established in the European Union may carry out transactions in a currency of a third country.[57]

Border restrictions and declaration

There are currently no border restrictions or requirements to declare cryptocurrency holdings when entering the Netherlands. Individuals carrying liquid assets such as cash to the value of €10,000 or more must declare this to Dutch Customs on entering the Netherlands from a country outside the European Union. However, cryptocurrencies are not regarded as cash for these purposes, and therefore it is currently not mandatory to declare cryptocurrencies when entering the Netherlands.[58]

Reporting requirements

There are currently no reporting requirements for cryptocurrency payments made in excess of a certain value. Cryptocurrency providers, however, need to submit suspicious reporting activity to our regulator based on the Dutch AML Act.

Estate planning and testamentary succession

There are no specific rules in the Netherlands as to how cryptocurrencies are treated for purposes of estate planning and testamentary succession. Accordingly, general civil law rules apply. With regard to the asset status, cryptocurrencies qualify as intangible assets (*immateriële activa*) for civil law purposes and as such, cryptocurrencies should be included in estate planning and testamentary succession, or form part of the estate.[59]

As cryptocurrencies are (intangible) assets, they are subject to inheritance tax.[60] The rate depends on the value of the inheritance, including the value of the cryptocurrencies, and the relationship between the heirs and the deceased.[61]

From the perspective of the heirs, it is particularly important that cryptocurrencies are specifically mentioned in the deceased person's estate and that they have, or will gain access to, the private key. Without access to the private key, the heirs will not be able to access the cryptocurrencies. Therefore, it is advisable from an estate planning perspective to deposit the private key with a notary in order to ensure that cryptocurrencies are not left behind in the wallet. If the cryptocurrencies are kept in an (online) account with an intermediary, it is also possible for the heirs to gain access to the wallet and the cryptocurrencies via that intermediary.[62]

* * *

Endnotes

1. Including tokens.
2. https://www.parlementairemonitor.nl/9353000/1/j4nvgs5kjg27kof_j9vvij5epmj1ey0/vkvcqggx2qz9/f=/kst32013201.pdf
3. https://www.rijksoverheid.nl/documenten/kamerstukken/2020/03/31/kamerbrief-nederlandse-reacties-op-eu-consultaties-cyberweerbaarheid-financile-sector-en-crypto
4. https://www.cpb.nl/nederland-moet-de-bitcoin-in-de-ban-doen
5. https://www.rtlnieuws.nl/economie/beurs/artikel/5235948/hoekstra-verbod-bitcoin-reactie-oproep

6. https://www.dnb.nl/en/innovations-in-payments-and-banking/everything-you-should-know-about-cryptos
7. M. Zeegers, "*Bitcoin; juridische en fiscale aspecten in beeld*", *WFR* 2015/329.
8. DNB "*Cryptoactiva: evolutie en beleidsrespons*", accessible via: rapport (dnb.nl).
9. IOSCO (International Organization of Securities Commissions) (2022). Decentralised finance report: Public report.
10. Zetzsche, D. Buckley, R.P. Arner, D.W. and Föhr. L. (2019). "The ICO Gold Rush: It's a scam, it's a bubble, it's a super challenge for regulators". *Harvard International Law Journal*, 60(2), pp 267–315.
11. Momtaz, P.P. (2020). Initial Coin Offerings. PLoS ONE 15(5): e0233018.
12. European Securities and Markets Authority (2019). Advice on Initial Coin Offerings and Crypto-Assets. ESMA50-157-1391.
13. Financial Stability Board (2022). Assessment of risks to financial stability from crypto-assets.
14. International Monetary Fund (2021). The crypto ecosystem and financial stability challenges. Global Financial Stability Report, chapter 2.
15. Financial Stability Board (2022). Assessment of risks to financial stability from crypto-assets.
16. DNB "*Cryptoactiva: evolutie en beleidsrespons*", accessible via: rapport (dnb.nl).
17. https://www.afm.nl/en/nieuws/2017/nov/risico-ico
18. Article 5:3 Financial Supervision Act.
19. Paul-Willem van Gerwen op Amsterdam Propriety Trading-event: "*Opkomst en populariteit van cryptoderivaten heeft onze aandacht*" (May), AFM.
20. DNB "*Cryptoactiva: evolutie en beleidsrespons*", accessible via: rapport (dnb.nl).
21. AFM and DNB, "Cryptos: recommendations for a regulatory framework", December 2018, p. 9.
22. Directive (EU) 2018/843 of the European Parliament and of the Council of 30 May 2018 amending Directive (EU) 2015/849 on the prevention of the use of the financial system for the purposes of money laundering or terrorism financing, and amending Directives 2009/138/EC and 2013/36/EU.
23. The UK Financial Conduct Authority ("**FCA**") and the Swiss Financial Market Supervisory Authority ("**FINMA**") use a similar categorisation.
24. AFM and DNB, "Cryptos: recommendations for a regulatory framework", December 2018, p. 9.
25. The definition of a financial instrument is set out in Article 1:1 Financial Supervision Act.
26. Implementation by the Markets in Financial Instruments Directive.
27. https://www.consilium.europa.eu/en/press/press-releases/2022/06/30/digital-finance-agreement-reached-on-european-crypto-assets-regulation-mica
28. Overheid.nl, "*Consultatie Uitvoeringswet Vo bij geldovermakingen en overdrachten van cryptoactiva te voegen informatie*" (internetconsultatie.nl); "*Crypto's grotendeels buiten toezicht AFM*"; Markets in Crypto-Assets Regulation ("**MiCAR**"); Charco & Dique (charcoendique.nl); and MiCAR (europa.eu).
29. 32545: *Brief van de minister van financiële markten 21 december 2022, stand van zaken omtrent de regulering van crypto's*.
30. https://www.businessinsider.nl/4-grootste-veranderingen-voor-consumenten-nieuwe-cryptowet-mica-bitvavo
31. Article 5.2 Income Tax Act 2001.

32. *Brief van de Staatssecretaris van Financiën van 28 mei 2018*, 2018-0000082316.
33. E. toe Laer, "*Welke waarde moet ik aanhouden voor bitcoins in de aangifte inkomstenbelasting*?", *FD* 9 March 2018.
34. Article 5.3 Income Tax Act 2001.
35. Article 3.90 Income Tax Act 2001.
36. https://www.kvk.nl/geldzaken/belasting-betalen-over-cryptos
37. Article 2.10 Income Tax Act 2001.
38. Article 3.2 Income Tax Act 2001.
39. https://www.belastingdienst.nl/wps/wcm/connect/nl/werk-en-inkomen/content/cryptovaluta
40. Article 22 Corporate Tax Act.
41. https://www.belastingdienst.nl/wps/wcm/connect/bldcontentnl/belastingdienst/zakelijk/winst/vennootschapsbelasting/veranderingen-vennootschapsbelasting-2022/tarief-2022
42. CJEU 22 October 2015, C-264/14, *Hedqvist*; VAT guidelines para. 759.
43. CJEU 22 October 2015, C-264/14, *Hedqvist*; VAT guidelines para. 759.
44. CJEU 22 October 2015, C-264/14, *Hedqvist*; VAT guidelines para. 759.
45. A. Hovansjan, A.Langedijk, "Navigating Dutch tax and financial regulatory on NFTs", *Lexology*.
46. Directive 2015/2366/EU of the European Parliament and of the Council of 25 November 2015 on payment services in the internal market.
47. https://www.dnb.nl/media/cz3fjb4f/explanatory-notes-to-the-form-for-registration-as-a-crypto-service-provider.pdf
48. (Co-)policymakers of crypto-asset service providers include persons actually (co-) determining the policy, management board members, and supervisory board members.
49. Court of Rotterdam, 7 April 2021, ECLI: RBROT:2021:2968.
50. *Boete voor Binance Holdings Ltd. vanwege het zonder de wettelijk vereiste registratie aanbieden van cryptodiensten* (dnb.nl).
51. W.J.M. Jansen and T.A. Keijzer, "*Tussen munt en mogelijkheid De ondernemingsrechtelijke aspecten van bitcoin*", WPNR 2022/7362 and Mr. M. van Ingen and Mr. W. Smits, "*Beslag op bitcoin: (praktisch) onmogelijk*", *Beslag, executie & rechtsvordering in de praktijk*, SDU nr. 2, April 2018.
52. W.J.M. Jansen and T.A. Keijzer, "*Tussen munt en mogelijkheid De ondernemingsrechtelijke aspecten van bitcoin*", WPNR 2022/7362.
53. T. de Graaf, "*De kwalificatie van bitcoins*", NJB 2019/2; H. Jongen *et al*., Blockchain 2022. Netherlands. Law and Practice, *Chambers and Partners Practice Guides* and W.J.M. Jansen and T.A. Keijzer, "*Tussen munt en mogelijkheid De ondernemingsrechtelijke aspecten van bitcoin*", WPNR 2022/7362.
54. M.G. van de Langemheen and Y.A. Wehrmeijer, "*Cryptovaluta: niet onaantastbaar*", Bb 2022/3.
55. J.P. Trespalacios and Justin Dijk, "The carbon footprint of bitcoin", DNB n.v. 2021.
56. *Bitcoin mining voor de BTW een economische activiteit, Fiscaal up to Date* (futd.nl).
57. ECLI:NL:RBDHA:2021:10751.
58. https://www.belastingdienst.nl/wps/wcm/connect/nl/bagage/content/geld-meenemen-op-reis
59. M.M.M. van Eechoud, J. Ausloos, M.B.M. Loos, C. Mak, B.E. Reinhartz, "*Data na de dood - juridische aspecten van digitale nalatenschappen (Onderzoek in opdracht van het Ministerie van Binnenlandse Zaken en Koninkrijksrelaties)*", University of Amsterdam, April 2021, p. 39.

60. L.A.G.M. van der Geld, "*De executeur in een nalatenschap met bitcoins en andere digitale bezittingen*", *Tijdschrift Erfrecht* 2014/6, p. 126.
61. https://www.belastingdienst.nl/wps/wcm/connect/nl/werk-en-inkomen/content/cryptovaluta
62. M.M.M. van Eechoud, J. Ausloos, M.B.M. Loos, C. Mak, B.E. Reinhartz, "*Data na de dood - juridische aspecten van digitale nalatenschappen (Onderzoek in opdracht van het Ministerie van Binnenlandse Zaken en Koninkrijksrelaties)*", University of Amsterdam, April 2021, p. 39.

Ilham Ezzamouri
Tel: +31 10 2488 063 / Email: ilhamezzamouri@eversheds-sutherland.com
Ilham is an experienced associate at Eversheds Sutherland and specialises in data protection, IT and privacy. Ilham has studied law at Erasmus University and the University of Amsterdam. Ilham has worked for national and international clients and has been seconded to several companies, including a European payment company. Prior to joining Eversheds Sutherland, Ilham worked as legal counsel in the field of privacy compliance and IT.

Robbert Santifort
Tel: +31 68 1880 472 / Email: robbertsantifort@eversheds-sutherland.com
Robbert is a principal associate specialised in new technologies and data privacy. He also has a strong focus on copyright law, e-commerce and trade secret protection. Robbert has extensive experience with IP/IT contracts and disputes, (international) data transfers and analysis, (data protection) compliance/enforcement issues and new technologies, such as big data analytics, blockchain and AI.

Eversheds Sutherland

Strawinskylaan 957, Tower Ten, 9th Floor, 1077 XX Amsterdam, Netherlands
Tel: +31 20 5600 600 / URL: www.eversheds-sutherland.com

Norway

Ole Andenæs, Snorre Nordmo & Karoline Angell
Wikborg Rein Advokatfirma AS

Government attitude and definition

General overview and attitude

The market for virtual assets and currencies has been growing rapidly in Norway over recent years, according to the Financial Market Report for 2023 by the Norwegian Ministry of Finance (**MoF**).[1] In the post-pandemic era, Norwegian consumers have actively sought new investment opportunities as they adapt to the changing times. While cryptocurrencies have gained significant attention, their volatility has made people more sceptical about their reliability over time.

The Norwegian market has been impacted by the volatile global crypto-asset market over the past year. This period witnessed value fluctuations, system failures, and bankruptcies. Notably, the collapse of FTX, along with the challenges faced by stablecoins such as USD Terra and USDC, has had a profound effect on investors, especially non-professionals. Furthermore, some banks catering to the crypto industry have also encountered problems.[2]

According to a recent survey conducted in April 2023 by K33 in collaboration with EY, approximately 8 per cent of Norwegian adults, equivalent to 345,000 individuals, own cryptocurrency. This figure indicates a decline of 2 per cent compared to the number of cryptocurrency investors in 2022.[3]

Among the providers of cryptocurrency services, we have witnessed a development of marketplaces and fund platforms for investments in virtual currency for selling, buying and making payments in cryptocurrencies or other digital assets with suitable fiat gateways. In addition, there has been a great deal of attention paid to developments in virtual assets based on blockchain technology, i.e., the market for non-fungible tokens (**NFTs**). According to the 2023 survey by K33 and EY, 23 per cent of Norwegian crypto owners are active in NFTs as of April 2023. This is an increase of 13 per cent from 2022.[4]

Government discussions have varied between whether to embrace or limit cryptocurrency. On the one hand, several regulatory issues have been raised due to lack of regulation and the potential risk factors associated with virtual currency, especially from a consumer perspective. Significant challenges have also been identified for both companies and individuals related to the practical handling of cryptocurrency and decentralised platforms both legally and fiscally. Ambiguities surrounding bookkeeping, reporting, and the proper classification of legal and tax requirements further compound the risks at hand, demanding careful and strategic approaches to mitigate them effectively.

The Financial Supervisory Authority of Norway (**FSAN**) has repeatedly warned against the risk of buying cryptocurrency and has addressed the strong need for a legal framework

and regulation of the crypto-asset market, stating that investor protection is crucial if cryptocurrency is to become a suitable form of investment for consumers.[5]

However, the government has demonstrated a constructive stance towards the exploration and utilisation of blockchain technology to unlock future technological advancement and stimulate new business models and markets – both within the private sector and the public domain.

Moreover, the government's attention has been directed towards the potential of financial products and services that use decentralised finance (**DeFi**). These innovative solutions have the capacity to limit the reliance on centralised third parties, leading to a reduction in brokerage costs and enhanced accessibility to financial services. Importantly, in specific contexts, DeFi solutions can offer heightened security by mitigating counterparty and settlement risk. The government has also addressed the legal challenges in the intersection between the General Data Protection Regulation (**GDPR**) and blockchain technology.

Government programmes

The Central Bank of Norway (**Central Bank**) reports that according to surveys conducted, only 3–5 per cent of Norwegians used cash for their last payment.[6] This makes Norway one of the most cashless societies in the world. It has therefore been argued that Norwegian consumers might be adaptable to alternative payment solutions, including DeFi solutions, virtual currencies and digital money.

The Central Bank has initiated a project to investigate whether to introduce a central bank digital currency (**CBDC**) by the end of 2025, which is widely available e-money issued by a central bank in the official monetary unit.[7]

CBDC represents a claim on the Central Bank, in the same way as banknotes and coins do today. The background for the project is the decrease in the use of physical cash and the possibility of major structural changes in the monetary and payment system, and where the issue of CBDC ensures that the public can continue to pay efficiently and securely in Norwegian kroner in the years ahead.[8] The Central Bank is also involved in the "Icebreaker" project, where the Norwegian Central Bank, the Sweden's Riksbank, the Bank of Israel and BIS Innovation Hub joined forces to test cross-border payments using CBDC.[9]

Commercial adaptation

Norwegian crypto companies provide services such as cryptocurrency payment technology, crypto and digital asset liquidity provisions, interbank trading platforms, crypto-fiat exchange, custody and brokerage services (both retail and institutional) and crypto hedge funds. There are currently nine entities registered with FSAN to provide exchange and storage of cryptocurrency in Norway.

Norges Bank Investment Management (**NBIM**) does not have the mandate to invest directly in cryptocurrency; however, the Norwegian oil fund holds indirect exposure through its ownership in various listed companies holding cryptocurrency on their balance sheet.

While cryptocurrency-related companies remain a relative small segment of the Norwegian financial market, a few players have emerged on the stock exchanges. Crypto/blockchain company Harmonychain is listed on the Oslo Stock Exchange (**OSE**). Harmonychain and its fully owned subsidiaries (Lokotech AS and Arctic Core AS) develop hardware and proprietary software dedicated to the crypto industry. OSE listed company Univid (formerly DLTx) withdrew from its blockchain initiatives and sold off its foreign operating subsidiaries in April 2023, including its involvement in Filecoin, to enhance its financial position as a consequence of the downturn in the blockchain market last year.[10]

In 2022, Norwegian full-service crypto company Arcane Crypto split into two businesses – Arcario, a web3 venture builder listed on Nasdaq First North Growth Market (retaining the original portfolio mandate), and K33, consolidating multiple portfolio companies creating a wealth management platform for digital assets.[11]

Norwegian Block Exchange (**NBX**) is a Norwegian cryptocurrency exchange, custodian and payment system registered with FSAN and is listed on Euronext Growth (a multilateral trading facility (**MTF**) operated by OSE). The company introduced the first Nordic Visa credit card with Bitcoin rewards, where the rewards will be saved directly to the card holders' dedicated NBX account.

Blockchain technology

The government has been largely positive to the development of blockchain technology for the delivering of information as it provides immediate and transparent information stored on an immutable ledger that can only be accessed by permissioned network members. The method of securely transferring values over the internet was originally developed to support digital currency; however, it can also be used for other purposes, such as in the finance and insurance industry and public administration.

In Norway, several projects have commenced involving blockchain technology among private and public actors. For example, DNV Group (owned by Stiftelsen Det Norske Veritas) and Deloitte have cooperated in a project to use blockchain to revitalise trust in the seafood industry by using a secure private blockchain for the storage of management systems, products and supply chain certificates, allowing anyone to obtain instant confirmation that a certificate is valid and up to date.[12]

Norwegian banks have raised the issue of customers transferring money derived from investments in, or trading in, cryptocurrency, where banks would be required to conduct surveys on the origin of funds (anti-money laundering (**AML**), know-your-customer process (**KYC**), etc.). As the authorities have defined the money laundering risk to be high in connection with cryptocurrency, banks are required to carry out thorough investigations. As a result, mortgage loan applicants who want to use monetary equity that originates from cryptocurrency investments to finance the purchase of properties have experienced that their loan applications are being rejected. Banks, such as Norway's largest bank, DNB, have emphasised that cryptocurrency is legal, and no customers should be declined or denied the establishment of a customer relationship solely based on their association with cryptocurrency. Nevertheless, it is crucial for banks to conduct thorough customer due diligence in the KYC process, which can be challenging, especially when dealing with the source of funds obtained through crypto-asset transfers.[13]

Cryptocurrency regulation

Financial regulatory framework

Currently, there is no legislation or regulatory framework in Norway specifically relating to cryptocurrency or blockchain technologies. However, there are a number of laws that apply to activities and services based on blockchain technology and virtual currencies.

Norway is not a member of the EU; however, Norway is part of the European Economic Area (**EEA**), which was established through the EEA Agreement. The EEA Agreement links Norway to the EU's internal market and forms the foundation of Norway's European policy. EU legislation does not automatically transform to Norwegian law, but must be incorporated into the EEA Agreement and subsequently be transposed into Norwegian law.

In Norway, Act no. 75 of 29 June 2007 on Securities Trading (**Securities Trading Act**), Act no. 23 of 1 June 2018 relating to Measures to Combat Money Laundering and Terrorist Financing (**AML Act**) and Act no. 17 of 10 April 2015 on Financial Institutions (**Financial Institutions Act**) partly regulate investments, customer due diligence, financial services and utility tokens.

Providers of exchange service platforms and custodian wallet providers of virtual currency are covered by the requirements of the AML Act, *cf*. the Anti-Money Laundering Regulations (**AML Regulations**). Such services can only operate after having been registered with FSAN, as further described below.

On 29 June 2023, Regulation (EU) 2023/1114 on Markets in Crypto Assets (**MiCAR**) entered into force in the EU, but the regulation encompasses a significant number of level 2 and level 3 measures that need to be formulated before the new regime takes effect (within a 12 to 18-month timeframe, depending on the mandate). The first batch of regulation will apply in the EU from 30 June 2024 and the second batch from 30 December 2024.

The MiCAR framework is part of the so-called "Digital Finance Package" (which also includes the Digital Operational Resilience Act (**DORA**) and the DLT Pilot Regime), which seeks to support innovation and competition in digital finance, in combination with risk-reducing measures for consumers and investors.

Throughout the implementation phase of MiCAR, the European Supervisory Authorities, ESMA, EBA, EIOPA, as well as the European Central Bank, are working together to engage in a public consultation on a series of technical standards to be published in three successive packages.[14]

MiCAR regulates instruments that are currently not covered by other EU regulations such as Directive 2014/65/EU on Markets in Financial Instruments (**MiFID II**) or the Directive 2009/110/EC on Electronic Money (**EMD II**). The new legal framework regulates transparency, disclosure, authorisation and supervision of transactions in the above-mentioned crypto-assets. MiCAR introduces harmonised rules for the issuance and public offering of stablecoins, such as ARTs and EMTs, in addition to requirements to draw up, notify and publish a crypto-asset white paper (**CA-WP**) for other crypto-assets. MiCAR expands the definition of what constitutes a crypto-asset service provider (**CAS-Provider**), and the provision of crypto-asset services is subject to licensing requirement. CAS-Providers can provide crypto-asset services throughout the EEA, either through the right of establishment, including through a branch, or on a cross-border basis (upon notification). Furthermore, more detailed rules are also given on supervision and administrative sanctions.

In the Financial Market Report for 2023, the MoF stated that MiCAR is considered EEA-relevant and that it is expected that the Ministry will assess Norwegian implementation once the regulations have been adopted in the EU. The market participants who will come under the new regulation according to the proposal are only partially subject to special rules today, in that the AML laws include providers of exchange services between virtual currency and official currency, and storage services for virtual currency. At the time of writing, there is no information available from the EEA committee nor the Norwegian legislator regarding the implementation of MiCAR, and the timeline for the entry into force of MiCAR and level 2 and 3 regulations (once adopted) in Norway is therefore uncertain.

Personal data

Act no. 38 of 15 June 2018 on Personal Data incorporating the GDPR applies to blockchains containing personal data. Some key issues arising are: (i) whether the storage of personal data

on a blockchain implies the processing of data; (ii) clarifying the responsibility of stakeholders for any GDPR non-compliance; (iii) safeguarding individuals' rights; and (iv) the need to undertake a data protection impact assessment prior to the use of blockchain technology.

One example is that blockchains represent a recorded transaction (which might violate the GDPR's "right to be forgotten") (Article 17(1) of the GDPR) and an individual has a right to demand the erasure of his/her personal data upon the withdrawal of consent, or upon his/her objections to the processing. The "right to be forgotten" can, however, be overridden by the controller's legal or legitimate ground to process the personal data (e.g., legitimate interest of the owners/operators of blockchain to comply with legal obligations).

Registration obligation

Exchange service platforms and custodian wallet providers of virtual currency must register with FSAN if the provider is: (i) registered in Norway; (ii) operating from Norway; or (iii) aiming the business towards the Norwegian market.

The registration obligation includes services such as: (i) offering customers to trade or exchange a type of virtual currency into an official currency (e.g., to Norwegian kroner, or *vice versa*); (ii) offering customers to switch between different types of virtual currencies (e.g., between Bitcoin and Ethereum); (iii) facilitating trade and exchanges by connecting buyers and sellers (e.g., through a platform); and (iv) storing private cryptographic keys on behalf of others, for the purpose of trading, transferring or storing virtual currency.[15] All exchanges between different virtual currencies, as well as between virtual currency and official currencies from all countries, are covered. This applies regardless of the form of payment, i.e., whether virtual currency is bought/sold with credit cards, cash, e-money, etc. Storage solutions that do not store private cryptographic keys (often referred to as "non-custodial wallets") are not covered by the regulations.

Service providers are covered by the regulations by virtue of the services they offer, regardless of how the service is organised. It is the activity itself that is the basis for the registration obligation.

Sales regulation

In contrast to regulated savings and investment products, there is no statutory consumer protection for buyers of cryptocurrencies in Norway at present. Crypto-assets covered by MiCAR will be regulated in Norway upon Norwegian implementation of the new framework.

FSAN has made it clear that until regulations on investor protection are adopted by the EU and the EEA, and eventually implemented in Norway, consumers especially must be aware of the potential risks associated with buying and selling cryptocurrency,[16] as investments in Bitcoin, for example, are volatile.

In March 2022, the European Financial Supervisory Authorities, ESMA, EBA and EIOPA, published a joint statement reminding consumers of the high risk associated with investment in Bitcoin, other virtual currencies or financial instruments exposed to such currencies.[17] FSAN supported the joint statement and published a new national warning in March 2022.[18]

Furthermore, FSAN published a press release in August 2021 stating that some cryptocurrency platforms in Norway have advertised on their websites that they are regulated by, or are approved by, FSAN, which FSAN emphasised as very misleading. The platforms have a duty to notify FSAN in accordance with the AML Regulations, but beyond money laundering supervision, FSAN does not supervise these actors.[19]

In June 2022, FSAN published a report on consumer protection and financial services in which the risks associated with cryptocurrency have been described in further detail.[20]

Taxation

Tax

The Norwegian tax authorities have found that, for tax purposes, virtual currency shall not be considered an ordinary currency because it is not issued or guaranteed by a central bank, and there is no formal issuer or official currency rate (as the price is determined by supply and demand). Virtual currency such as cryptocurrency, digital tokens and other digital values are considered, for tax purposes, as assets. As a result, income from virtual currency follows the general tax rules for assets, and gains and income are calculated as capital income (currently taxed at 22 per cent). Cryptocurrencies are not covered by exemptions or special tax rules that apply to ordinary (fiat) currency, shares, bonds, financial instruments or other types of assets with special exemption rules.[21]

The taxation requirement applies whether virtual currency is sold, bought, mined or stored. Each individual or company must determine the value of, and report and document, gains, losses, dividends and assets in the tax return.[22]

Creating an NFT (minting) does not trigger taxation. However, all income related to an NFT is generally taxable, including creator/issuer or other rightful owner's income that is a result of the resale of an NFT.[23]

The Norwegian Tax Administration has identified approximately 180,000 individuals in Norway who owned cryptocurrencies in 2021, but they estimate that the actual number is much higher. The tax authorities observe that a significantly larger number of individuals are declaring ownership of cryptocurrencies compared to previous years. In 2021, 42,781 individuals reported owning cryptocurrencies, compared to 15,251 in 2020. The reported income amounted to NOK 9.8 billion, representing an increase of NOK 8.8 billion from the previous year, while the reported wealth was NOK 23 billion, up from NOK 8 billion in 2020.[24]

Upon sale or other realisation of virtual currency, there will be a taxable gain or deductible loss. Gains/losses on realisation constitute the difference between the input value and the output of the current virtual currency, adjusted for any costs associated with the transaction. Furthermore, it is required to be able to present documentation to authorities upon request. Tax declaration shall be declared in Norwegian kroner, meaning that the value must be converted into Norwegian kroner if originally transferred in another currency.

It should be noted that the same tax rules and principles apply to DeFi products (e.g., Uniswap, Compound, Yearn and Aave) as to virtual currency, meaning that all income is taxable; for example, swap/exchange of cryptocurrency and tokens or returns from participation in liquidity pools, etc.[25]

Valued-added tax (**VAT**)

The Court of Justice of the European Union ruled in C-264/14 (*Hedqvist*)[26] that Bitcoin must be on the same footing as other traditional currencies in regard to the exception in Article 135(1)(e) of Directive 2006/112. The MoF made a statement on 6 February 2017 that if the EU ruling must be taken into account in Norway, transactions of Bitcoin or other cryptocurrencies will comprise the financial exception in Article 135(1)(e) of Directive 2006/112.[27] As a result, transactions made with or related to cryptocurrencies are exempted if payment in cryptocurrency is agreed upon by the parties as an alternative means of payment, and do not have any other purpose.

In a binding advanced ruling of 6 February 2018, the Norwegian Tax Administration assessed that an enterprise that only sells computing power to others for the mining of

virtual currency must calculate VAT. The ruling, however, cannot be interpreted as a definitive position on whether mining of cryptocurrency can be subject to exemption from VAT for financial services.[28]

The obligation to pay tax and VAT in connection with ICOs must be assessed individually and on a case-by-case basis. With regard to VAT, it must be assessed whether the ICO can be considered a financial service based on whether there is a supply of goods or services, and if so, what has been supplied.

Money transmission laws and anti-money laundering requirements

Even though typical cryptocurrencies would not fall within the definition of e-money, as e-money involves a "claim on the electronic money issuer", some crypto-assets may fall under the definition of e-money in the Financial Undertakings Act § 2-4. E-money can only be issued by banks, mortgage companies and e-money undertakings and by finance undertakings that are licensed to conduct such activities in Norway. The Central Bank is of the opinion that both technical and regulatory barriers prevent the use of stablecoins for traditional payments. Since stablecoins are often implemented as tokens on open blockchains, capacity constraints and fees in the blockchains limit the attractiveness of such stablecoins for mass payments. In 2022, the Central Bank emphasised that new scaling solutions can effectively mitigate this issue in the future.[29] This viewpoint has not been further pursued by the Central Bank in 2023, as it shifted its focus more towards the volatility in the cryptocurrency markets during 2022.[30] MiCAR will, once implemented in Norway, regulate issuers of stablecoins, both ARTs and e-money tokens, as well as all other crypto-assets and service providers.

The AML Act and Regulations implement the EU's fourth and fifth AML Directives. The AML Act applies to exchange services and custodian wallet providers. Pursuant to § 1-3 of the Norwegian AML Regulations, the regulations apply to businesses that are registered in the Norwegian Business Register, as well as others operating from Norway, or even service providers aiming their currency exchange services at the Norwegian market. FSAN has clarified that it is the activity of providing services to the Norwegian market that is the foundation of applying such register obligations, rather than formalities such as the place of registration.[31]

In July 2021, the European Commission presented a package of legislative proposals in the area of AML efforts and countering the financing of terrorism.[32] One of the proposals aims to extend the EU regulation on traceability in electronic payments (Regulation (EU) 2015/847) to also apply to transfers of cryptocurrencies. Norway and the other EEA/EFTA states (Iceland and Liechtenstein) have expressed support to reinforce the AML and counter-terrorist financing framework *vis-à-vis* the EU, but they have expressed scepticism regarding direct supervision through the Anti-Money Laundering Authority at European level.[33] A provisional agreement was reached between the Council presidency and the European Parliament on transparency of crypto-asset transfers on 29 June 2022. This includes that Member States will have to ensure that all CAS-Providers qualify as obliged entities under the fourth AML Directive in due course.[34]

Promotion and testing

FSAN has established a "regulatory sandbox" for the purpose of increasing innovation within the fintech industry in order to facilitate for new actors and increased competition.[35]

At the time of writing, we have not seen any examples of providers of crypto services participating in the existing sandbox or a specific sandbox targeting DeFi. However, the fintech company Abendum participated in the regulatory sandbox in 2021 with a service for storing and making available audit evidence based on blockchain technology.[36]

Norway is also part of a partnership of all EU Member States, Norway and Liechtenstein and the European Commission, building a European Blockchain Services Infrastructure (**EBSI**). As part of this EU/EEA blockchain community, a European blockchain regulatory sandbox has been set up to provide a pan-European regulatory framework, enhancing legal clarity for inventive blockchain solutions and fostering innovation with distributed ledger technologies (**DLT**).[37]

In addition to several private initiatives, we have seen a number of public entities/agencies in Norway initiating projects to assess the potential benefits of blockchain technology.

One example is Brønnøysund Register Centre's (the national register in Norway) aim to connect ownership registries through a blockchain-based solution, using the BRØK platform, for publishing ownership information. This enables other service providers, financial institutions, media, and government agencies to access and read information without the need for APIs or complex development work.

BRØK is a new service currently under development that utilises blockchain technology to enable the sharing of information about a company's shareholders. In BRØK, a new version of the shareholder registry is not published when changes occur. Instead, individual changes in the shareholder registry are published, creating an audit trail.[38]

Additionally, there have been other notable initiatives such as Verse Gallery, situated in Oslo, renowned as Scandinavia's pioneering permanent physical gallery exclusively dedicated to NFT-supported digital art.[39]

Ownership and licensing requirements

In Norway, a quasi-regulatory regime applies for virtual currency exchange and virtual currency safekeeping. A virtual currency is defined as a digital representation of value, not issued by a central bank or other public authority (i.e., not money), but which is accepted as a method of payment and which may be transferred, stored or traded electronically.

Currently, Norwegian cryptocurrency providers are not required to obtain a licence, except for the obligation to register with FSAN. However, this scenario is set to evolve with the forthcoming implementation of MiCAR in Norway.

FSAN supervises whether actors offering cryptocurrency to the Norwegian market comply with registration requirements, general suitability requirements and the AML laws.

FSAN has also stated that service providers must be registered in the Norwegian Business Register in order to be registered as providers of exchange services and virtual currency storage services in Norway. Furthermore, it is assumed that the operation of services will take place via a separate company account. As a consequence, the actors must establish a Norwegian entity or branch with a Norwegian organisation number in order to be registered in the Business Register. So far, the nine registered providers of exchange services and virtual currency storage services in Norway are Norwegian private limited liability companies or sole proprietorships, and currently we have not seen any registration of Norwegian branches of foreign entities. In 2021, it was announced that Binance had stopped trading and making payments in Norwegian kroner, dropped Norwegian websites,

and will no longer have an official communication channel in Norwegian after they received a formal inquiry from FSAN.[40]

FSAN may reject applications that do not meet the requirements of the AML Act, if the information that accompanies the registration request is incomplete or if the beneficial owners, directors, general managers and other persons involved in the actual management of the business are not considered fit and proper. It is not permitted to start exchange or storage services for virtual currency until FSAN has made a positive decision on the registration.

With regard to ownership of virtual assets, it is only the holder of the private key who can possess and transfer the assets, and the legal qualification of virtual assets remains uncertain. One of the topics that has been discussed by the Central Bank is accountability of decentralised systems. One method of imposing responsibility on decentralised systems is to open up new forms of organisation that can be held accountable, e.g., so-called "decentralised autonomous organisations" (**DAOs**), such that, in accordance with regulations, legal personal status can be granted on an equal footing with companies and other legal entities.[41] Currently, such organisational forms are not specifically regulated in the Norwegian jurisdiction (and such organisations would most likely constitute partnerships under current Norwegian company law).

Mining

There are currently no restrictions or bans on the mining of cryptocurrencies, although there have been political and legislative discussions on whether data farms and other facilities mining Bitcoin and other cryptocurrencies should pay full electrical fees. The government discontinued reduced electricity tax for data centres and cryptocurrency mining in connection with State Budget 2023.[42]

Border restrictions and declaration

There are no specific border restrictions or declarations required when importing cryptocurrencies into Norway as cryptocurrencies are not considered money. Individuals carrying cash exceeding NOK 25,000 must declare this to Norwegian Customs; however, as cryptocurrencies are not considered cash, these restrictions do not apply.

To apply the main rule concerning the transaction value of imported goods, the price that has been actually paid or is going to be paid for the goods must be known. Payment made with, for example, virtual currency is not considered to fulfil the requirement of a known price and is not accepted as a basis for applying the main rule of the transaction value.[43]

Reporting requirements

There are currently no specific reporting requirements for crypto-assets in Norway, other than the reporting requirements under the AML Regulations and tax regulations as previously described.

Estate planning and testamentary succession

Norway has no explicit legislation addressing how crypto-assets should be treated in the context of estate planning and testamentary succession. Cryptocurrency and crypto-asset accounts are considered personal property that will fall into the estate of the deceased, and will therefore be subject to testamentary succession and the distribution of the estate. See further information on tax implications above.

Endnotes

1. https://www.regjeringen.no/contentassets/2f9e7828fa724306afb815f10885a53d/no/pdfs/stm202202300180000dddpdfs.pdf
2. https://www.norges-bank.no/contentassets/1af9f294a4724f2faa9e6759c3516d36/finansiell-infrastruktur-2023.pdf?v=05/25/2023130358
3. https://assets.ey.com/content/dam/ey-sites/ey-com/no_no/news/news-2023/ey-k33-norwegian-crypto-survey-2023.pdf
4. See note 3.
5. https://www.finanstilsynet.no/nyhetsarkiv/nyheter/2022/de-europeiske-finanstilsynsmyndighetene-minner-om-risikoen-ved-virtuell-valuta
6. https://www.norges-bank.no/contentassets/1af9f294a4724f2faa9e6759c3516d36/finansiell-infrastruktur-2023.pdf?v=05/25/2023130358
7. https://www.norges-bank.no/contentassets/1af9f294a4724f2faa9e6759c3516d36/finansiell-infrastruktur-2023.pdf?v=05/25/2023130358
8. https://www.norges-bank.no/contentassets/554ee1f1ac53417d99d43708f5abbe14/norges-bank-memo-1-2021.pdf?v=06/07/2021092959
9. https://www.bis.org/about/bisih/topics/cbdc/icebreaker.htm
10. https://www.digi.no/artikler/paskedrama-i-kryptoselskap/529188
11. https://k33.com/about
12. https://www2.deloitte.com/ie/en/pages/about-deloitte/articles/Deloitte_DNV_GL_first_blockchain_solution_certification_industry.html
13. https://www.dnb.no/dnbnyheter/no/meninger/hvorfor-ma-bankene-kjenne-sine-krypto-kunder-
14. https://www.esma.europa.eu/esmas-activities/digital-finance-and-innovation/markets-crypto-assets-regulation-mica
15. https://www.finanstilsynet.no/konsesjon/virtuelle-valutatjenester
16. https://www.finanstilsynet.no/nyhetsarkiv/nyheter/2021/forbrukere-og-kryptovaluta
17. https://www.eba.europa.eu/eu-financial-regulators-warn-consumers-risks-crypto-assets
18. https://www.finanstilsynet.no/nyhetsarkiv/nyheter/2022/de-europeiske-finanstilsynsmyndighetene-minner-om-risikoen-ved-virtuell-valuta
19. https://www.finanstilsynet.no/nyhetsarkiv/nyheter/2021/finfluensere-og-forbrukervern
20. https://www.finanstilsynet.no/contentassets/d3dd2ba101194c64b6513dd63e602303/forbrukervern-og-finansielle-tjenester.pdf
21. https://www.skatteetaten.no/en/person/taxes/get-the-taxes-right/shares-and-securities/about-shares-and-securities/digital-currency/tax-regulations-virtual-currency
22. https://www.skatteetaten.no/en/business-and-organisation/reporting-and-industries/industries-special-regulations/internet/tax-and-vat-on-virtual-currencies
23. https://www.skatteetaten.no/en/person/taxes/get-the-taxes-right/shares-and-securities/about-shares-and-securities/digital-currency/nft
24. https://www.nettavisen.no/nyheter/stadig-mer-kryptovaluta-rapporters-i-skattemeldingen/s/5-95-1036016
25. https://www.skatteetaten.no/en/person/taxes/get-the-taxes-right/shares-and-securities/about-shares-and-securities/digital-currency/defi
26. https://curia.europa.eu/juris/liste.jsf?num=C-264/14
27. https://www.regjeringen.no/no/dokumenter/merverdiavgift---unntaket-for-finansielle-tjenester/id2538129
28. https://www.skatteetaten.no/en/business-and-organisation/reporting-and-industries/industries-special-regulations/internet/tax-and-vat-on-virtual-currencies

29. https://www.norges-bank.no/contentassets/7437af41dbd94dbfaee9e7f0d231a3ba/finansiellinfrastruktur_2022.pdf?v=05/20/2022091846&ft=.pdf
30. https://www.norges-bank.no/contentassets/1af9f294a4724f2faa9e6759c3516d36/fi_2023_0106.pdf?v=06/02/2023122604
31. https://www.finanstilsynet.no/konsesjon/virtuelle-valutatjenester
32. https://ec.europa.eu/info/publications/210720-anti-money-laundering-countering-financing-terrorism_en
33. https://www.regjeringen.no/contentassets/2f9e7828fa724306afb815f10885a53d/no/pdfs/stm202220230018000dddpdfs.pdf
34. https://www.consilium.europa.eu/en/press/press-releases/2022/06/29/anti-money-laundering-provisional-agreement-reached-on-transparency-of-crypto-asset-transfers
35. https://www.finanstilsynet.no/tema/fintech/finanstilsynets-regulatoriske-sandkasse
36. https://www.finanstilsynet.no/nyhetsarkiv/nyheter/2022/sluttrapport-fra-abendum-etter-deltakelse-i-finanstilsynets-regulatoriske-sandkasse
37. https://ec.europa.eu/digital-building-blocks/wikis/display/EBSI/Sandbox+Project
38. https://beta.brreg.no/forside/brok
39. https://www.versegallery.xyz/en
40. https://e24.no/teknologi/i/EaJjga/verdens-stoerste-kryptoboers-kutter-i-norge-etter-brev-fra-finanstilsynet
41. https://www.norgesbank.no/contentassets/7437af41dbd94dbfaee9e7f0d231a3ba/finansiellinfrastruktur_2022.pdf?v=05/20/2022091846&ft=.pdf
42. https://www.regjeringen.no/no/aktuelt/avvikler-redusert-elavgift-for-datasentre-og-kryptoutvinning/id2930646
43. https://www.toll.no/no/verktoy/regelverk/handboker/vareforselshandboken/6/6-3

Ole Andenæs
Tel: +47 22 82 76 61 / Email: oea@wr.no

Ole Andenæs is a Partner at Wikborg Rein's Oslo office and heads the firm's Financial Regulations practice.

Andenæs previously worked as Head of Legal in investment bank Carnegie AS, and he has in-depth and practical knowledge about the regulatory framework surrounding investment firms, asset managers, investor behaviour and adjacent regulations. Prior to this, Andenæs worked as a Senior Lawyer at the law firm Thommessen, where he mainly worked with financial regulations, advising a wide range of regulated entities, as well as company law and disputes within these areas. He is also a specialist in company law, and is the co-author of "*Aksjeselskaper og allmennaksjeselskaper*" (3rd edition 2016) ("*Public and Private Limited Company Law*").

Snorre Nordmo
Tel: +47 22 82 76 09 / Email: sno@wr.no

Snorre Nordmo is a Partner at Wikborg Rein's Oslo office and is part of the firm's Capital Markets practice.

Snorre is specialised in asset management and financial regulatory matters and has broad experience within the industry from both a service provider and client perspective. He advises both regulated and unregulated asset managers, including investment firms, alternative investment managers (within private equity, hedge funds, real estate, private debt, infrastructure, etc.), securities fund managers, investment banks and financial institutions, pension funds, insurance companies, family offices, consultants, advisers and service providers within the asset management industry. Snorre has previously worked as General Counsel at Sector Asset Management (the largest hedge fund manager in Norway) and as an Attorney at Norges Bank Investment Management (NBIM, the manager of the Norwegian sovereign wealth fund).

Karoline Angell
Tel: +47 22 82 75 10 / Email: ang@wr.no

Karoline Angell is a Senior Associate at Wikborg Rein's Oslo office and is part of the firm's Asset Management and Financial Regulatory practice. Karoline works primarily with financial regulatory issues and securities law, and has particular experience with issues related to anti-money laundering regulations. This includes advising Norwegian and foreign regulated entities on matters related to licensing, operation and organisation of activities in line with applicable laws and regulations.

Wikborg Rein Advokatfirma AS

Dronning Mauds gate 11, PO Box 1513 Vika, NO-0117 Oslo, Norway
Tel: +47 22 82 75 00 / URL: www.wr.no

Poland

Mihhail Šerle
Gofaizen & Sherle Sp. z o.o.

Government attitude and definition

Polish law has defined virtual currency as a digital image of value that is not considered fiat money, electronic money, a financial instrument, a promissory note or a cheque and is accepted as a means of exchange with an option to be electronically stored, transferred or the subject of electronic trade. The Polish government does not intend to become involved in the issuance of any virtual currencies, and such currencies cannot be used as a means of payment for interactions with government (e.g. payment of taxes, state fees, etc.). Nevertheless, fulfilling payment obligations in virtual currency is permitted if parties agree on such means.

Virtual currencies and services related thereto are not supervised by the Polish Financial Supervision Authority (PFSA) and no notices have been issued to make such statements available to the public. Nevertheless, PFSA has issued some guidelines and recommendations related to virtual currencies, the most recent of which helped to qualify virtual currencies and distinguish them from financial instruments in the context of Polish financial supervision. Recent guidelines have distinguished currency/exchange tokens, utility tokens and investment/security tokens, as well as combinations of them.

It is important to note that virtual currency service providers (VCSPs) are currently not considered part of the financial market within the meaning of Polish law. The Polish legislative framework on virtual currency services is not comprehensive and there is no direct supervision of VCSPs by PFSA.

Cryptocurrency regulation

In accordance with Polish anti-money laundering (AML) law, virtual currency services may be provided by natural persons and legal entities that meet the following requirements:

- The entity must have established internal policies (AML/KYC), as well as internal control policies.
- The entity must appoint a qualified employee who is responsible for the fulfilment of AML and counter-terrorism financing (CTF) obligations as specified in AML law.
- The entity must have all the necessary procedures for the establishment and monitoring of business relationships and identification of customers who benefit from the services of the company.
- The entity must implement all the necessary procedures for fulfilment of international sanctions.
- The entity must install the necessary infrastructure for the safe storage of customer data and implement appropriate security measures to protect against cyber threats and unauthorised access to such data.

- Procedures for reporting suspicious transactions and other operations should be applied.
- The entity is obliged to implement a risk-based approach in the course of its activity, taking into account the risks identified through relevant risk assessments.

Natural persons and senior managers of VCSPs must not have been convicted of certain crimes (including for the purpose of material or personal gain or an intentional fiscal offence). This requirement shall be proven by the absence of a criminal record, or, depending on which jurisdiction is the place of residence of the applicant, an oath that the applicant has no convictions.

In addition, a senior manager of a VCSP shall have the necessary experience and qualifications, such as:

- completion of training or a course covering legal or practical issues related to virtual currencies; or
- experience in the field of virtual currencies for a period of at least one year, proven by relevant documents.

Although these requirements seem transparent, Polish law does not always assess the applicant's experience and in practice, a person's written confirmation in the application is considered suitable means for fulfilment of the above requirements.

The crucial requirement for VCSPs is entering into the Polish Register of Virtual Currency Activities (*Rejestr działalności w zakresie walut wirtualnych*). This defines Polish jurisdiction from others due the obligation not only to meet common AML obligations following the EU's 5th AML Directive, which sets the grounds for provision of the abovementioned services, but to follow the strict rules necessary to access the Polish market. In other words, even trustworthy entities that, at the first glance, meet the main requirements of the EU Directive cannot operate in Poland until its entrance in the abovementioned Register, operated by the Polish tax authority (the National Revenue Administration).

To enter into the Register, the established entity must fill in an application containing the following information:

- name and surname or the company name;
- number in the register of entrepreneurs in the National Court Register, if assigned, and tax identification number;
- information on the virtual currency services provided; and
- a qualified electronic signature, trusted signature or personal signature of the applicant.

After the information is received, the National Revenue Administration should make registration publicly available within 14 days. It is important to note that there is no specific licensing procedure, and the registrar does not control a VCSP's compliance with AML/CTF requirements (e.g. existence of procedures, etc.) in the course of the registration process.

AML regime compliance is supervised by the General Inspector of Financial Information (GIFI) of the Minister of Finance Department of Financial Information (*Ministerstwo Finansów Departament Informacji Finansowej – Generalnego Inspektora Informacji Finansowej*).

Taxation

Cryptocurrency transactions are subject to taxation in Poland. The country treats cryptocurrencies as taxable assets, and individuals and businesses are required to report cryptocurrency-related income and gains for tax purposes. The specific tax rates depend on the type of transaction and the individual's or company's tax status.

Money transmission laws and anti-money laundering requirements

Polish AML law and requirements for obliged entities are applicable to VCSPs. Furthermore, Poland has implemented the requirements of the 5th AML Directive, which are also applicable to VCSPs and detailed below.

The obligation to apply customer due diligence measures includes the following:

- identification of a customer (and its representative) and verification of its identity;
- identification of a beneficial owner and undertaking justified measures to verify its identity and define the ownership and control structure;
- identifying whether a customer or person(s) related to a customer are politically exposed persons (PEPs), including their family members and close associates;
- assessment of a customer's business relationship and, as applicable, obtaining information concerning its objective and intended nature;
- ongoing monitoring of a customer's business relationship, including analysis of transactions carried out throughout the course of the business relationship to ensure that such transactions are compliant with the knowledge of the obligated institution on the customer, the type and scope of activity carried out by it, and with the money laundering and financing of terrorism (ML/TF) risk associated with such customer. Examining the origin of assets available to the customer may be justified in certain circumstances; and
- ensuring that documents, data and information concerning the business relationship are updated on an ongoing basis.

VCSPs are obliged to apply customer due diligence measures in the following cases:

- when establishing a business relationship;
- when performing operations with virtual currencies in the amount of EUR 1,000 or its equivalent in other assets;
- when there is a suspicion of ML/TF; and
- when there are doubts regarding the authenticity or completeness of a customer's identification data.

Poland has no specific requirements for customer identification procedures, and the law only establishes requirements to collect certain data about customers (name or business name, date of birth, registry code, etc.).

Polish AML law has no specific requirements for crypto transaction monitoring. There are also no travel rule requirements for transactions with virtual currencies.

In addition to the above, VCSPs must comply with AML/CTF regulations, including:

- Suspicious transaction reporting: If a VCSP becomes aware of or suspects any transaction that may be related to ML/TF, they are obligated to report it to the Polish Financial Intelligence Unit (FIU). A VCSP must promptly notify the FIU of any suspicious transactions, even if they are in the process of verifying the suspicion.
- Record-keeping: Providers must maintain records of all transactions and customer information for a specific period of time (five or 10 years, depending on the type of information). These records should be easily accessible to regulatory authorities upon request.
- Internal controls: VCSPs are expected to establish and maintain effective internal controls, policies, and procedures to prevent ML/TF. This includes implementing risk-based systems to monitor and detect suspicious transactions.

Failure to comply with these reporting requirements can result in penalties and legal consequences. It is important for VCSPs to understand and adhere to AML/CTF regulations and regularly update their compliance procedures as per the evolving regulatory landscape.

In order to meet the reporting and other requirements provided by the AML regime, VCSPs must appoint a qualified employee (AML Officer) to be responsible for the fulfilment of AML/CTF obligations as specified in AML law.

There is a statutory and regulatory obligation on a company to disclose information to the AML Officer in circumstances where they:

- identify any circumstances that may indicate the suspicion of ML/TF;
- become suspicious that the specific transaction or assets may be associated with ML/TF; or
- become suspicious that the assets subject to transaction or collected on the account originate from or are associated with a crime other than ML/TF or from a fiscal crime.

In addition, the AML Officer:

- conducts ongoing monitoring of the company's relationships with it customers and reviews such monitoring on a regular basis;
- identifies suspicious transactions and activities;
- monitors changes in regulatory requirements with respect to ML/TF prevention and counteraction and communicates all AML/CTF-relevant issues to the responsible senior management member(s);
- develops internal training programmes and materials and receives relevant training; and
- performs other functions that are assigned to the AML Officer under applicable law, internal policies, and job description.

Promotion and testing

Poland has, indeed, taken steps to establish a favourable environment for fintech companies and blockchain startups. The country has embraced the development of digital technologies and has made efforts to encourage innovation in the fintech industry, while the Polish government has implemented various initiatives and programmes to promote the growth of fintech and blockchain startups. For instance, PFSA, the regulatory body overseeing the financial sector, has launched a regulatory sandbox. This sandbox allows fintech companies to test their innovative solutions in a supervised environment, without the burden of strict regulations. The aim is to foster innovation while maintaining consumer protection. Nevertheless, this initiative is mostly aimed at financial market participants and not VCSPs.

Additionally, Poland has implemented the "Startup Poland" initiative, which seeks to enhance the development of startups, including those in the fintech and blockchain sectors. This initiative offers support through mentorship, access to funding, networking opportunities, and other resources to help startups thrive.

In terms of cryptocurrencies, Poland's approach has been cautious. The Polish government has shown concerns regarding the potential risks associated with cryptocurrencies, such as money laundering or funding illegal activities. As a result, there have been several regulatory measures meant to ensure transparency and consumer protection.

While Poland has not implemented specific programmes or initiatives to encourage investment in the cryptocurrency sector, the regulatory environment strives to strike a balance between fostering innovation and mitigating risks. The overall aim is to create a secure and regulated environment for cryptocurrency-related activities.

Please note that the situation and policies can evolve, so it is essential to stay updated on the latest regulations and initiatives in Poland's fintech and blockchain sectors.

Mining

There are no specific regulations prohibiting or restricting cryptocurrency mining activities in Poland. However, it is important to note that the operation of mining facilities may be subject to general regulations regarding electricity consumption, land use, or environmental protection. It is advisable for miners to comply with applicable laws and regulations related to these areas. Additionally, miners are expected to comply with taxation requirements and report any income generated from mining activities to the relevant authorities.

Border restrictions and declaration

There are no specific border restrictions or obligations to declare cryptocurrency holdings when entering or leaving Poland. Cryptocurrencies are not considered legal tender in Poland, and there are no specific regulations requiring individuals to declare their cryptocurrency holdings at the border. However, it is essential to stay updated on any changes in regulations or requirements, as cryptocurrency laws and regulations are constantly evolving. It is also worth noting that individuals travelling to other countries should research and comply with the cryptocurrency regulations of their destination country, as some countries may have specific requirements or restrictions in place.

Reporting requirements

The AML Officer is responsible for submitting external reports to the GIFI and for keeping track of all internal investigations and escalations, which may be reproduced in writing.

The submission of external reports of suspected ML/TF shall not:

- allow for attributing a lower risk of ML and TF to the customer;
- allow the company to limit the application of customer due diligence measures;
- exempt the company from applying enhanced due diligence measures; or
- exempt the company from the obligation not to conduct transactions through the bank account or to terminate business relationships with the customer should it be unable to apply customer due diligence measures.

The VCSP must report the following information (amount-based reports) through the AML Officer to the GIFI:

1. accepted payments or executed withdrawals of virtual currency exceeding the equivalent of EUR 15,000;
2. executed transfers of virtual currency exceeding the equivalent of EUR 15,000 (with some exemptions); and
3. executed purchase and sale transactions of foreign currency with a value exceeding the equivalent of EUR 15,000, or intermediation in performing such transaction.

Suspicious transactions

In addition to amount-based reports, VCSPs should report suspicious transactions. Suspicious transactions shall be identified:

- by noting the activities of customers that, by their nature, may be related to ML/TF;
- when conducting the customer's and beneficial owner's identification; and
- when conducting ongoing monitoring of the business relationship, including the investigation of transactions that have occurred during that relationship.

Suspicious transaction reports to the GIFI shall be made using the relevant reporting template. Reports to the GIFI should be sent via its website (https://www.giif.mofnet.gov.pl) or, in exceptional cases, by email.

The AML Officer plays an active role in the identification and reporting of suspicious transactions. Principal functions of the AML Officer include, in particular:

- reviewing all internal disclosures and exception reports and determining whether it is necessary to report to the GIFI;
- maintaining all records related to such internal reviews;
- providing guidance on how to avoid "tipping off" if any disclosure is made; and
- acting as the main point of contact with the GIFI, law enforcement, and any other competent authorities in relation to ML/TF prevention and detection, investigation or compliance.

In addition to suspicious activity reports and currency transaction records, Poland provides for an obligation to report infringements. Any VCSP employee or other persons performing activities for the VCSP (reporting person) who become(s) aware of real or potential infringements of the provisions in the scope of AML/CTF by employees or other persons performing activities for the VCSP shall report the aforementioned conduct (i.e. an infringement report) using the infringement report form. The infringement report may only be done in good faith. It is prohibited to knowingly make a false infringement report. Reporting persons who act for a purpose contrary to law or the principles of social cohabitation do so in bad faith.

Whistleblower officers are responsible for receiving and investigating infringement reports and for collecting infringement reports and personal data of the reporting person or persons suspected of committing an infringement in a separate database. The entity shall process personal data pursuant to the provisions of Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of individuals with regard to the processing of personal data and on the free movement of such data and repealing Directive 95/46/EC (GDPR).

Estate planning and testamentary succession

In Poland, the treatment of cryptocurrencies for estate planning and testamentary succession purposes is still a developing area of law. At the time of writing, there are no specific regulations in place that directly address cryptocurrencies in the context of estate planning and testamentary succession.

However, the general principles of Polish inheritance law would apply to cryptocurrencies as they would to other types of assets. This means that cryptocurrencies can be included in a person's estate and distributed according to their will or the rules of intestate succession if no will exists.

To ensure the smooth transfer of cryptocurrencies upon death, it is advisable to include specific provisions in a will or create a separate document that outlines the details of the digital assets and provides necessary instructions for their transfer. It may be helpful to specify the cryptocurrency holdings, digital wallets, and any relevant access information to facilitate the transfer of the assets.

Mihhail Šerle
Tel: +48 222 304 095 / Email: mihhail@gofaizen-sherle.com

Mihhail Šerle, a native of Tallinn, Estonia, graduated from Tallinn University. He has been a practising lawyer since 2012 and holds a Master of Laws degree. Over the past three years, Mihhail has specialised in corporate law and AML/CTF compliance.

Mihhail has comprehensive knowledge and experience in most European jurisdictions. His main area of legal activity is the establishment of companies and obtaining the authorisation of a virtual currency service provider and he currently specialises in the Polish market.

Mihhail possesses extensive experience in structuring internal documents and frameworks, catering to both small businesses and large financial institutions. His paramount concern during service provision is ensuring the client's successful commencement of business operations while maintaining optimal compliance with local jurisdiction. Mihhail diligently addresses the nuances of clients' activities, assisting in the effective establishment of essential business processes.

Gofaizen & Sherle Sp. z o.o.

Hoża 86, 00-862 Warsaw, Poland
Tel: +48 222 304 095 / URL: www.gofaizen-sherle.com

Portugal

Filipe Lowndes Marques, Vera Esteves Cardoso & Ashick Remetula
Morais Leitão, Galvão Teles, Soares da Silva & Associados

Foreword

For the purposes of this chapter, we will be addressing blockchain and crypto-assets as the latter encompasses several types of assets, including cryptocurrency.

The term "crypto-assets" shall be used interchangeably with the term "virtual assets" since the latter corresponds to the legal wording in the Portuguese jurisdiction for such type of assets (without prejudice to the upcoming laws and regulations that may come into force following the enactment of Regulation (EU) No. 2023/1114 on markets in crypto-assets ("**MiCA**")).

Government attitude and definition

Government attitude

Blockchain technology (or distributed ledger technology, "**DLT**") in general, and crypto-assets in particular, are closely followed topics in the fintech industry not only within the Portuguese ecosystem but also among the Government and the relevant regulatory authorities.

In recent years, Portugal has become one of the main European crypto hubs, attracting considerable amounts of investment and also founders, entrepreneurs, investors and other market players. Blockchain and crypto-assets have gained momentum considering the rise of the digital services era, market capitalisation of the crypto industry, with a steady increase in the adoption of crypto-assets, emergence of new blockchain-based business models across several industries (e.g., art, entertainment, finance, gaming, real estate, sports), increase in the level of investment from mature and more sophisticated market players, and potential increase in the scope of regulation, even more so with the recently published MiCA.

Institutional developments include:

i. **Virtual Asset Service Providers**: Law No. 83/2017, of 18 August, as amended, on anti-money laundering and combatting the financing of terrorism ("**Portuguese AML Law**"), sets forth the general regime applicable to the authorisation and registration, for purposes of anti-money laundering and combatting the financing of terrorism ("**AML/CFT**"), of Virtual Asset Service Providers ("**VASPs**"), together with the notices issued by the Portuguese Central Bank ("**Bank of Portugal**"),[1] in line with the European Union ("**EU**") regulatory framework.
ii. **Portugal FinLab**: an innovation hub/communication channel between market players and the Portuguese regulatory authorities (banking, securities and insurance) through which the authorities provide guidelines on how to navigate and operate in the regulatory system. The purpose of Portugal FinLab is to support the development of innovative solutions in fintech and related fields (which include DLT/blockchain and crypto-assets) through cooperation and mutual understanding.

iii. **Regulatory Sandboxes**: Decree-Law No. 67/2021, of 30 July, sets the framework for the creation of regulatory sandboxes (designated "**Technological Free Zones**").[2] The envisaged sandboxes intend to create "safe spaces" in which companies can test innovative products, services and business models without immediately incurring all the normal regulatory consequences related to the activity. Any entity that wishes to apply to create a Technological Free Zone must file an application or submit a declaration of interest on the website of the National Innovation Agency and follow the relevant formal procedure.[3]

iv. **National Blockchain Strategy**: the development of a national strategy for blockchain is on the Government's agenda, in line with Portugal's "Action Plan for Digital Transition". The Government and regulatory authorities have been invested in studying DLT (including blockchain) and crypto-assets with a view to creating favourable conditions for the establishment and development of the sector, while protecting all market participants' interests and also considering that there is a large base of Portuguese users participating in crypto-asset transactions and/or investing in crypto-assets.

v. **Real Estate "Purchase"**: the Portuguese Notary Association (a public professional association) announced last year that an internal regulation would be published to regulate real estate acquisitions made using crypto-assets, in cases where they are not converted into legal tender.[4]

vi. **DLT Regime**: Decree-Law No. 66/2023, of 8 August, implemented EU provisions on the use of DLT to issue, trade and settle financial instruments issued through DLT, namely in regard to the issuance of debt instruments. The provisions set forth address the technological challenges linked to the financial disintermediation triggered by the use of DLT, including the form of representation and registration.

vii. **Blockchain-based Registry of Intellectual Property Rights**: in July 2023, Portugal joined the EU project for the blockchain integration of the EU Intellectual Property Office-associated intellectual property registration platforms.

These new technologies have inevitably drawn the attention of the relevant regulatory authorities, most notably the Bank of Portugal, the Portuguese Securities and Markets Commission ("**CMVM**")[5] and the Portuguese Insurance and Pension Funds Supervisory Authority ("**ASF**").[6]

Notably, both the Bank of Portugal and the CMVM, in their capacity as both central bank and national competent authority for the supervision of credit and payment institutions on the one hand and, on the other hand, the national competent authority for the supervision of securities market, have shown a clear interest in crypto-assets, in particular from the perspective of consumer/investor protection, since the early days of the crypto boom. Both authorities have issued a number of public statements, notices and warnings in relation to crypto-assets, in line with the regulatory practices of other central banks of the EU and European regulatory authorities, such as the European Banking Authority ("**EBA**") and the European Securities and Markets Authority ("**ESMA**").

Furthermore, both the Bank of Portugal and the CMVM have also created a dedicated page on their website, addressing crypto-asset matters and their regulation, and a specific email for people to address any issue related with these assets, and in the CMVM's case, other matters related to the fintech industry.

As an interesting fact, in 2018, the Government issued a token – GOVTECH – that was used to cast votes by allocating those tokens to competing projects, thereby replicating investment choices, in a technological competition sponsored by the Government. The initiative was the first of its kind in Portugal and demonstrates the Government's openness to new technologies.

Definition

Portugal closely follows the rules arising from the EU legislative procedure. Without prejudice to some minor amendments that the national regulations may set forth, the general principles and definitions are guided by EU legislation (some of which is automatically applicable in Portugal, without the need for transposition).

Taking the above into account, the definitions set forth under national law closely follow those adopted at EU level.

Furthermore, it is noteworthy that, considering the recent publication of MiCA and its entry into force in the near future, the definitions related to crypto-assets in general and the specific types of crypto-assets will follow the definitions set forth under that regulation (or national laws and regulations that are expected to come into force to densify those new rules).

Without prejudice to the abovementioned, in the Portuguese jurisdiction, in relation to blockchain/DLT, the following definitions have been adopted:

i. **Distributed Ledger**: an information repository that keeps records of transactions and is shared across, and synchronised between, a set of DLT network nodes using a consensus mechanism.
ii. **DLT**: a technology that enables the operation and use of distributed ledgers.

Both the aforementioned definitions are derived from Regulation (EC) No. 2022/858 on a pilot regime for market infrastructures based on DLT ("**DLT Pilot Regulation**"), which was further developed nationally by the aforementioned Decree-Law No. 66/2023, of 8 August, and are also adopted under MiCA. There is no specific definition covering blockchain in particular (neither in national nor EU laws and regulations).

On the other hand, concerning crypto-assets, we note the following definition:

i. **Virtual Asset**: a digital representation of value that is not necessarily linked to a legally established currency and does not have the legal status of a fiat currency, security or other financial instrument, but which is accepted by natural or legal persons as a means of exchange or investment and can be transferred, stored and traded electronically.

In respect to specific normative definitions, this is the only one that can be found in the Portuguese jurisdiction under the Portuguese AML Law, which transposed Directive (EU) No. 2018/843 on AML/CFT ("**AMLD5**").

Further to the above, despite not being specifically addressed by Portuguese laws and regulations, it is worth highlighting the following definitions set forth under MiCA that will soon be adopted by EU Member States:

i. **Crypto-asset**: a digital representation of value or of a right that is able to be transferred and stored electronically using DLT or similar technology.
ii. **Asset-referenced Token**: a type of crypto-asset that is not an e-money token and that purports to maintain a stable value by referencing another value or right or a combination thereof, including one or more official currencies.
iii. **E-money Token**: a type of crypto-asset that purports to maintain a stable value and referencing the value of one official currency.
iv. **Utility Token**: a type of crypto-asset that is only intended to provide access to a good or a service supplied by its issuer.

Apart from above, in respect to security tokens, there are no specific laws or regulations designed to address them. As is common in other countries, the approach taken is to consider that tokens that may be qualified as a security, taking into account its characteristics, shall be treated as such and subject to Portuguese securities laws and supervised by the CMVM.

This qualification is to be conducted on a case-by-case basis and, in general, the token will fall under that scope if it represents one or more rights and obligations and in relation to which the token holders are entitled to an income (e.g., return on investment).

The origin of this approach to security tokens dates back to 2018, when the CMVM issued a formal notice addressed to all entities involved in initial coin offerings ("**ICOs**")[7] regarding the legal qualification of tokens. The CMVM stressed the need for all entities involved in ICOs to assess the legal nature of the tokens being offered under the ICOs, in particular their possible qualification as securities with the application of securities laws as a consequence. The CMVM noted that tokens can represent different rights and credits, and can be traded in organised markets, thus concluding that tokens can be qualified, on a case-by-case basis, as (atypical) securities under Portuguese law, most notably considering the broad definition of securities provided under the Portuguese Securities Code.

Furthermore, non-fungible tokens ("**NFTs**") do not usually fall under the scope of virtual assets, as established under the Portuguese AML Law, nor are some of them covered by the provisions of MiCA. There are no specific national regulations addressing NFTs. However, existing legal regimes apply to the issuance, marketing and sale of such tokens, such as intellectual property, consumer protection, e-commerce, advertising laws and regulations, among other sectorial provisions depending on the characteristics of the NFT. In addition, please note that the issuance and sale/purchase of NFTs is usually regulated contractually by acceptance of terms and conditions published by the issuer.

In Portugal, crypto-assets do not have legal tender status and thus do not qualify as fiat currency.

Nonetheless, crypto-assets are largely seen as an alternative payment method with a contractual nature that results from a private agreement between participants of crypto-asset transactions, and with intrinsic characteristics that somewhat replicate some of the core traits of fiat currency: storage of value; unit of account; and medium of exchange. Taking this into consideration, contrary to other countries that have been developing trials for government-backed crypto-assets, including those that have successfully launched such assets, there is no public governmental proposal to provide legal backing to crypto-assets. Crypto-assets are thus not backed by the Government or the Bank of Portugal. However, please note that the envisioned Central Bank Digital Currency, namely the Digital Euro, despite aiming to be a crypto-asset, will not be subject to the same legal framework as other crypto-assets (namely MiCA).

Cryptocurrency regulation

At present, there are no specific laws or regulations that govern issues related to cryptocurrency (except the rules established in the Portuguese AML Law). However, with the enactment of MiCA and its direct applicability in Portugal in the near future as an EU Member State, this is likely to change.

Nonetheless, even without considering MiCA, one cannot say that there is a regulatory vacuum in this context, since existing laws will need to be assessed on a case-by-case basis to determine whether they apply to a particular crypto-asset or related activity. Hence, the laws and regulations applicable to crypto-assets will vary greatly depending on the specific characteristics of each token.

Portuguese AML Law

As mentioned above, the Portuguese law that specifically addresses services provided with crypto-assets (or virtual assets in the normative definition) is the Portuguese AML Law, which transposed AMLD5. This law sets forth a mandatory registration procedure for

persons (whether natural or legal) seeking to provide certain services to clients with virtual assets – so-called VASPs. Note, however, that this registration is mandatory for AML/CFT supervision purposes; hence, it is not the same as a standard licensing procedure carried out, for example, by a regulated financial entity.

According to said law, the following persons will have to be authorised and registered with the Bank of Portugal, prior to commencing their activity in Portugal, when the following activities are carried out for and on behalf of their customers:

i. providers engaged in exchange services between virtual assets and fiat currencies;
ii. providers engaged in exchange services between one or more forms of virtual assets;
iii. providers of services that allow the transfer of virtual assets from one address or wallet to another; and
iv. providers of custodian wallet services (which allow the safeguarding of private cryptographic keys on behalf of their customers, to hold, store and transfer virtual assets).

In a nutshell, exchange services, transfer services and custodian services in relation to virtual assets are specifically regulated for AML/CFT supervision purposes.

However, this authorisation and registration procedure is mandatory when the aforementioned services are exercised/operated within Portuguese territory. The following entities are considered to operate within Portuguese territory:

i. legal persons incorporated in Portugal to carry out activities with virtual assets;
ii. natural or legal persons with a domicile or establishment in Portugal engaged in activities with virtual assets; and
iii. natural or legal persons who, due to the exercise of activities with virtual assets, are obliged to submit a statement at the start of their activity to the Portuguese Tax Authority.

Securities laws and regulations

As mentioned above, some crypto-assets, due to their intrinsic characteristics, may potentially be qualified as securities and become subject to existing securities regulations, most notably regulations applicable to public offerings of securities and/or securities trading venues.

The CMVM has clarified the elements that may implicate the qualification of tokens as securities, namely:

i. if they may be considered documents (whether in dematerialised or physical form) that are representative of one or more rights of a private and economic nature; and
ii. if, given their particular characteristics, they are similar to typical securities under Portuguese law.

For the purpose of verifying the second point, the CMVM will take into account any elements, including those made available to potential investors (which may include any information documents, such as a white paper), that may entail the issuer's obligation to undertake any actions from which the investor may draw an expectation to have a return on its investment, such as:

i. granting the right to any type of income (e.g., the right to receive earnings or interest); or
ii. undertaking certain actions, by the issuer or a related entity, aimed at increasing the token's value.

Moreover, the CMVM also advised that where a token does not, or is not intended to, qualify as a security, its issuer should avoid the use, including in the token's documentation, of any expressions that may be confused with terms commonly used in securities markets, such as "investor", "investment", "secondary market" and "admission to trading".

For example, tokens that represent rights and/or economic interests in a pre-determined venture, project or company, such as tokens granting the holder a right to take part in the profits of a venture, project or company or even currency-type tokens, will, in principle, be subject to securities laws and regulations.

Since the Portuguese jurisdiction, namely the competent authorities, follow the rules and guidelines set by their EU counterparts, it is worth mentioning that ESMA's position regarding the regulatory implications when a crypto-asset qualifies as a financial instrument[8] has been adopted in Portugal. In the particular case of ICOs, in general, being subject to securities laws, ESMA provides advice on the potential application of, notably:

i. Directive No. 2003/71/EC ("**Prospectus Directive**");
ii. Directive No. 2013/50/EU ("**Transparency Directive**");
iii. Directive No. 2014/65/EU on markets in financial instruments ("**MiFID II**");
iv. Regulation (EU) No. 600/2014 on market in financial instruments ("**MiFID Regulation**") and respective implementing acts;
v. Regulation (EU) No. 596/2014 ("**Market Abuse Regulation**") and Regulation (EU) No. 236/2012 ("**Short-Selling Regulation**");
vi. Directive No. 2009/44/EC ("**Settlement Finality Directive**");
vii. Regulation (EU) No. 909/2014 ("**Central Securities Depository Regulation**"); and
viii. Directive No. 2011/61/EU on alternative investment fund managers ("**AIFM Directive**").

All of the abovementioned pieces of legislation have been transposed into the Portuguese jurisdiction, and the rules set forth therein are reflected namely in the Portuguese Securities Code.

In this context, if a token qualifies as a security, the relevant national and EU laws shall apply, including, *inter alia*, those related to: the issuance, representation and transmission of securities; public offerings (if applicable); marketing of financial instruments for the purposes of MiFID II; information quality requirements; and market abuse rules.

Finally, in the particular case of an ICO or Security Token Offering ("**STO**"), should they qualify as a public offering, a prospectus should be drafted and submitted, along with any marketing materials, to the CMVM for approval, provided that no exemption applies in relation to the obligation to draw a prospectus.

General laws and regulations applicable

As previously mentioned, the lack of specific laws and regulations addressing crypto-assets in particular does not mean that crypto-assets/tokens that are not subject to the laws and regulations referred to above are completely unregulated and navigating in the void.

Existing legal frameworks shall apply in accordance with the subject matter/characteristics of the crypto-asset/token/service at stake.

The following regimes may be applied to some crypto-assets/services, depending on the specific case at hand:

i. the Portuguese Civil Code;
ii. intellectual property laws in relation to the creation and licensing of underlying intellectual property rights;
iii. Regulation (EU) No. 2022/2065 ("**Digital Services Act**" or "**DSA**");
iv. Decree-Law No. 7/2004 ("**e-Commerce Law**");
v. consumer protection laws, notably Decree-Law No. 24/2014 ("**Distance and Off-Premises Law**") and Decree-Law No. 84/2021 ("**Digital Goods, Content and Services Law**");

vi. the Advertising Code; and
vii. other sector-specific rules that may applicable.

Finally, note that a party's autonomy always carries some weight; hence, parties may contractually agree on some rules where they do not contradict mandatory legal provisions.

Sales regulation

Considering the lack of exclusive regulation in relation to crypto-assets in Portugal, as described under "Cryptocurrency regulation" above, the sale and purchase of crypto-assets *per se* are also not specifically regulated.

However, to the extent that a crypto-asset/token sale may be qualified as, for example, an offer of consumer goods or services or an offer of securities to the public, the relevant existing laws and regulations on, respectively, consumer protection and securities and financial markets (including national laws that transposed, among others, the EU legislation mentioned above) may apply by default, including their sanctions regime, subject to, in any case, an individual assessment. In these cases, both consumer protection law and securities law provide a number of obligations that must be complied with during and after the sale process.

Therefore, existing regulations on the sale of consumers' goods or services and of securities can apply to certain types of tokens on a case-by-case basis, in accordance with an "as-applicable principle".

Taxation

Key outlook

The State Budget Law for 2023, which came into force in the beginning of this year, introduced specific tax on crypto-assets for the very first time. This represented a major turning point for the tax framework applicable to crypto-assets.

This recently approved crypto-asset tax regime can be split into the following main issues:
i. establishment of a normative definition of crypto-assets for tax purposes;
ii. taxation of income from transactions with crypto-assets;
iii. taxation of gratuitous transfers of crypto-assets;
iv. taxable value for property transfer tax purposes; and
v. taxation of commissions and fees charged by VASPs.

Moreover, this new Portuguese tax regime was approved and entered into force at the same time that new tax transparency rules were proposed by the European Commission for all VASPs for customers resident in the EU.

Additionally, this new regime also addresses the creation of reporting obligations for providers of crypto-asset custody and management services on behalf of clients or those that manage one or more crypto-asset trading platforms. Entities covered by these obligations will have to report to the Tax Authority all crypto-asset transactions carried out with their intervention.

Definition of crypto-assets for tax purposes

The legal definition of crypto-assets adopted in Portugal for tax purposes follows the definition that was established by MiCA (replicated above). The definition is intentionally very broad and intends to cover most types of crypto-assets, such as cryptocurrencies, stablecoins, utility tokens and security tokens. However, it expressly excludes "unique crypto-assets that are not fungible with other crypto-assets", meaning NFTs.

Taxation of income from transactions with crypto-assets

Personal Income Tax

For Personal Income Tax ("**PIT**") purposes, income that results from the issuance of crypto-assets or from the validation of transactions with crypto-assets through consensus mechanisms in the context of a business or professional activity will be taxed as business or professional income (Category B).

Furthermore, any form of income resulting from transactions with crypto-assets that is not qualified as business or professional income will qualify as investment income, taxable as PIT Category E income, subject to a flat rate of 28% and exempt from withholding tax, regardless of the form it takes. However, when the consideration takes the form of other crypto-assets, this income will be taxed under PIT Category G income as capital gains, but only at the moment of disposal of the crypto-assets.

Corporate Income Tax

For Corporate Income Tax ("**CIT**") purposes, the new rules provide that income that results from the issuance of crypto-assets or from the validation of transactions with crypto-assets through consensus mechanisms is considered income derived from commercial or industrial activities and is therefore subject to CIT.

Capital gains

Gains from the sale of crypto-assets are qualified as capital gains, taxable as PIT Category G income. However, the regime foresees two different scenarios with different treatments – one scenario where those gains are taxable and another where those gains are not taxable:

i. capital gains on crypto-assets held for less than one year are taxed at a flat rate of 28%; and
ii. capital gains on crypto-assets held for more than one year are excluded from taxation (not applicable to crypto-assets classified as securities).

If the disposal of the crypto-assets takes the form of other crypto-assets (i.e., crypto to crypto), the new regime establishes that the crypto-assets received are to be attributed the acquisition value of the crypto-assets delivered, hence deferring taxation (if applicable) to the moment when the capital gain is realised.

The above-mentioned exemption as well as the tax deferral will not apply when the taxpayer is not resident in an EU Member State, the European Economic Area or another country that does not have an agreement with Portugal to exchange information for tax purposes.

Taxation of gratuitous transfers of crypto-assets

It is also foreseen that the disposal of crypto-assets through gratuitous transfers (e.g., inheritance or donations), which do not generate any taxable capital gains, may be subject to stamp duty at a 10% rate.

The stamp duty will be levied on gratuitous transfers whenever:

i. the crypto-assets are deposited in institutions with a registered office, effective management or permanent establishment in Portuguese territory;
ii. the deceased was domiciled in Portugal, in inheritance cases; or
iii. the beneficiary is domiciled in Portugal, in the remaining operations.

The stamp duty should be paid, in principle, by the beneficiary of the gratuitous transfers. However, the exemption currently applicable to gratuitous transfers of other assets in favour of certain beneficiaries (e.g., spouses, unmarried partners, descendants and ascendants) also applies to gratuitous transfers of crypto-assets.

Taxable value for property transfer tax purposes

In case of an exchange of crypto-assets for real estate, the taxable value of the transaction for property transfer tax purposes – to determine the applicable tax rates – will be, in principle, the market value of the crypto-assets on the date of the transaction.

Taxation of commissions and fees charged by VASPs

Commissions and fees charged on transactions carried out by or with the intermediation of VASPs domiciled in Portugal or to customers domiciled in Portuguese territory are subject to a 4% stamp duty, which is borne by the customers. In case of non-payment, the new rules also foresee that the customer will be jointly and severally liable with the service provider for the payment of the tax.

Value-added Tax

The new tax regime is silent on the Value-added Tax ("**VAT**") implications of transactions with crypto-assets.

Until now, the interpretation of the Court of Justice of the European Union ("**CJEU**") and the binding rulings issued by the Tax Authority were the available landmarks relied on to assess the VAT treatment of transactions with crypto-assets.

In line with the CJEU interpretation of the VAT treatment of transactions with crypto-currencies, the Tax Authority ruled that transactions such as the exchange of crypto-currency for fiat currency (and *vice versa*) should be exempt from VAT.

The Tax Authority has published two official rulings in the context of certain requests for binding information relating to crypto-assets in the context of VAT (January and July 2019).[9,10] In the absence of other laws and regulations that may clarify the taxation regime of cryptocurrencies, these rulings have important weight and will work as precedents in relation to how the Tax Authority will look into crypto-assets and crypto-asset-related activities when interpreting existing tax provisions and deciding whether or not a certain fact or action should be subject to tax. In any event, as these were given in the context of requests for binding information, the Tax Authority may revoke these rulings in the future.

In the referred official rulings, the Tax Authority confirmed the precedent from the CJEU (Case C-264/14, *Skatteverket v. David Hedqvist*) to argue that although crypto-assets such as Bitcoin were analogous to a "means of payment" and therefore subject to VAT, they were exempt by application of VAT exemption rules, which should be consistent across EU Member States considering existing EU VAT harmonisation.

While this guidance on the exemption for the exchange of crypto-assets for fiat currency, and *vice versa*, can still be relied on, the new regime implies a new approach to the VAT treatment of transactions with crypto-assets. The full extent of the changes brought by the new rules is yet to be determined.

Working Paper No. 1060 on the VAT treatment of NFT transactions was issued in February 2023 by the EU VAT Committee and provides a good illustration of the complexity of determining whether or not a person or entity carrying out transactions with crypto-assets is a taxable person, the nature and corresponding VAT treatment of transactions with crypto-assets, and their place of supply and taxable amount, as well as different criteria adopted by different EU Member States.

Thus, practical application in the course of 2023 will be critical in gauging the impact of the new tax framework on the VAT treatment of transactions with crypto-assets.

Money transmission laws and anti-money laundering requirements

As previously mentioned, the Portuguese AML Law introduced a mandatory registration procedure for all VASPs that undertake their activity within Portuguese territory.

The Bank of Portugal has been the competent authority in registering and verifying compliance with the applicable legal and regulatory provisions governing AML/CFT by VASPs, being, at the time of writing and according to the public list published by the Bank of Portugal, 11 registered entities, five of which have not been authorised to commence activities. The registration procedure is regulated by the Bank of Portugal's Notice No. 3/2021, of 24 April.

It should be made clear, however, that in relation to VASPs, the Bank of Portugal's competence is limited to AML/CFT issues and does not extend to prudential, behavioural or other areas of supervision (this will most likely change with the enactment of new rules on the competent national authorities as foreseen under MiCA; however, it has not yet been determined which authority will supervise the various different types of entities who provide services with crypto-assets under the new rules).

According to the Portuguese AML Law, VASPs are now considered "obligated entities". This means that, under Portuguese law, VASPs are legally required to comply with all applicable AML/CFT legal dispositions, which include but are not limited to risk management, transaction monitoring, know-your-customer ("**KYC**") and due diligence obligations, adequate technical, material and human resources (which includes a specific Money Laundering Reporting Officer, or "**MLRO**") and a responsible board member with AML/CFT responsibilities.

In addition, VASPs must be aware that their type of activity entails the reinforcement of certain, more common identification procedures and that customer due diligence as an additional risk is presumed to exist in products or operations that favour anonymity, in new products or commercial activities, in new distribution mechanisms and payment methods, and in the use of new technologies or developing technologies.

Furthermore, more recently, the authority issued Notice No. 1/2023, of 24 January, covering matters foreseen in the Portuguese AML Law, the application and execution of restrictive measures approved by the United Nations or by the EU, and establishing the sanctions framework for breaches of said measures.

These advances indicate the increased level of regulation of the sector in question, which has been associated with considerable AML/CFT risk.

This new Notice is addressed to entities that develop activities with virtual assets within domestic territory, registered as such with the Bank of Portugal. Entities not registered in domestic territory are considered "entities of equivalent nature" and, while they are not directly subject to the provisions of this new Notice, the business relations between them and entities registered in domestic territory are thereby regulated in several aspects, namely in relation to the implementation of enhanced due diligence measures.

The Notice further aims to harmonise national legislation with the international framework on AML/CFT, pre-emptively including some of the content expected to be included in the EU AML Package (the legislative package aimed at AML/CFT), which is now in an advanced negotiation stage. It is also driven by Recommendation 15 of the Financial Action Task Force ("**FATF**"), reviewed in 2018 to include provisions on VASPs, as well as by the FATF's "Updated Guidance for a Risk-Based Approach to Virtual Assets and Virtual Asset Service Providers", published in 2021, as is evident, for example, in the inclusion of the travel rule in the Notice.

The goal of this Notice is to clearly define the procedures, tools, mechanisms, formalities and provision of information duties, among other aspects deemed necessary to the fulfilment of VASP-related AML/CFT duties, a sector that has been identified as high risk and in which entities have had less time to develop their experience in adhering to these duties, as the procedures associated with the registration of VASPs with the Bank of Portugal only entered into force on 24 April 2021, in line with the Explanatory Memorandum of this new Notice.

The Notice, articulated with the legal framework on AML/CFT, mainly aims to:

i. clarify how the provisions in the Portuguese AML Law and in Law No. 97/2017 apply to VASPs, taking into consideration particular risks and technical characteristics of the sector; and
ii. introduce innovative elements in this legal framework that are specific to the daily life of the VASP sector.

Concretely, this new Notice issued by the Bank of Portugal addresses the execution of preventive duties on AML/CFT by VASPs that are subject to the Bank of Portugal's supervision for AML/CFT purposes. The following provisions should be highlighted:

i. The duty to define and implement an AML/CFT control function. This function should be segregated from the activities it must monitor, with the exception of entities with less than six employees. This heightened internal control duty for AML/CFT purposes also includes the designation of an MLRO, which should take on such functions exclusively.
ii. Although it is now generally admissible, subcontracting of processes, services, or activities for complying with these duties is subject to a set of rules and limitations, including the VASP's responsibility for such subcontracting, the prohibition of subcontracting when it jeopardises the quality of the implemented measures, the duty to assess the underlying risks, considering AML/CFT preventive measures and the legal framework of the subcontracted entity, among others.
iii. Videoconferencing has also been introduced as a possible means of identity confirmation when performing customer due diligence in the terms set by Article 25 of the Portuguese AML Law. It can now be used both by VASPs and by subcontracted entities, when admissible, and upon compliance with several safeguards and technical and general requirements.
iv. Customer due diligence.
v. Provisions for greater control of the origin and destination of virtual assets are included, with certain information on the sender and the recipient mandatorily accompanying their transfers, following the travel rule proposed by the FATF in Recommendation 15.
vi. The duty to identify and evaluate specific risk factors for this sector is included, based on the assessment performed by the FATF.

The breach of preventive duties by VASPs may constitute an administrative offence.

Promotion and testing

The Government had initially launched a think tank with the objective of generally promoting and fostering fintech – mostly by identifying and targeting entry barriers – with the ultimate aim to implement a regulatory "sandbox" with the aid of the Portuguese financial regulators.

In 2018, a non-profit organisation, Portugal Fintech, and the main Portuguese regulators – ASF, the Bank of Portugal and the CMVM – joined efforts to create Portugal FinLab, which created a direct communication platform for emerging tech companies working in fintech-related subjects, incumbents, and Portuguese regulators to engage and to provide guidance on a clearer path of action in terms of the application of the existing regulatory framework to the activities of those companies.

Portugal Fintech, a non-profit fintech community created in 2016 in Portugal, has also been extremely active in this regard. It manages:

i. the Portugal Fintech Report, an annual report that contains data regarding the Portuguese fintech ecosystem and its development;
ii. Fintech House, launched in January 2020, which is a fintech hub – an ecosystem where every fintech, regtech, insurtech and cybersecurity company in Portugal can easily interact with regulators, legislators, consultants, banks, investors and other relevant entities; and
iii. Fintech Solutions, which is the advisory arm of Portugal Fintech, focused on closing the gap between startups and incumbents. Fintech Solutions builds customised projects for financial and non-financial institutions that seek to incorporate fintech startups in their services and processes, targeting proof of concepts as a strategy to achieve results.

Ownership and licensing requirements

As mentioned in "Cryptocurrency regulation" above, in Portugal, there are no specific restrictions or licensing requirements when it comes to purchasing, holding or selling crypto-assets from the user's perspective, except where they are qualified as securities. However, as mentioned in "Money transmission laws and anti-money laundering requirements" above, VASPs operating within Portuguese territory are required to obtain prior registration with the Bank of Portugal.

Furthermore, insofar as crypto-assets are not qualified as financial instruments, advisory services that are made exclusively in relation to, and the exclusive management of, crypto-asset portfolios are not subject to the same investment services laws and regulations as those applicable to securities.

However, traditional advisory services and management services require licensing and are subject to the CMVM's supervision.

Mining

There are no restrictions in Portugal on the development of mining of cryptocurrencies and the activity itself is not regulated.

Border restrictions and declaration

In Portugal, there are no border restrictions or obligations to declare crypto-asset holdings.

Reporting requirements

There is no standalone reporting obligation in case of crypto-asset payments above a certain threshold, except in the case of transactions that may involve an obliged entity covered by the Portuguese AML Law, in which case such entity will have to report suspicious transactions or activities irrespective of the amounts involved.

Estate planning and testamentary succession

There is no precedent, specific rules or particular approach regarding the treatment of crypto-assets for the purposes of estate planning and testamentary succession in Portugal.

Notwithstanding, certain aspects of estate planning and testamentary succession should be highlighted. Inheritance tax does not exist in Portugal, but stamp duty may apply to certain transfers of certain assets (e.g., immovable property, movable assets, securities and negotiable instruments, provided they are located, or deemed to be located, in Portugal) included in the deceased's estate in case of succession.

However, in the absence of a legal amendment or binding information from the Tax Authority, it may be argued that the drafting of the relevant legal provisions does not expressly foresee assets such as cryptocurrencies, thus excluding the same from the scope of application of stamp duty, which *de facto* mitigates the need for estate planning with respect to crypto-assets. Estate planning and testamentary succession must therefore be analysed on a case-by-case basis, considering all variables involved.

* * *

Endnotes

1. Please refer to the "Cryptocurrency regulation" section for further information.
2. From the Portuguese *Zonas Livres Tecnológicas*.
3. As of this date, the Government has approved the creation of two Technological Free Zones to (i) test and experiment products and services that intend to accelerate the transition to a carbon-neutral economy, and (ii) test and validate new communications, sensors, artificial intelligence and materials.
4. Legally speaking, this would not be considered a purchase deal (*compra-e-venda*) but an exchange deal (*permuta*).
5. In Portuguese, *Comissão do Mercado de Valores Mobiliários*.
6. In Portuguese, *Autoridade de Supervisão de Seguros e Fundos de Pensões.*
7. The CMVM's notice addressed to all entities involved in ICOs, dated 23 July 2018, available in Portuguese at https://www.cmvm.pt/pt/Comunicados/Comunicados/Pages/20180723a.aspx?v=
8. *Cf*. European Securities and Markets Authority, "Advice: Initial Coin Offerings and Crypto-Assets", dated 9 January 2019, available at https://www.esma.europa.eu/sites/default/files/library/esma50-157-1391_crypto_advice.pdf
9. *Cf*. *Autoridade Tributária e Aduaneira*, Binding Information provided in process No. 5717/2015, dated 27 December 2016.
10. *Cf*. *Autoridade Tributária e Aduaneira*, Binding Information provided in process No. 14763, dated 28 January 2019 and in process No. 14436, dated 3 July 2019.

Filipe Lowndes Marques
Tel: +351 213 817 400 / Email: flmarques@mlgts.pt

Filipe Lowndes Marques heads the banking and finance department at Morais Leitão. Filipe oversees and participates directly in all financial regulatory matters (notably fintech) dealt with by his team and is one of the main partners in charge of the firm's main fintech partnerships (Fintech House and Nova SBE fintech accelerator). Vastly experienced in project finance, he has worked on all kinds of projects since 1995, including bridges, highways, power plants, wind and solar farms, football arenas, LNG terminals and natural gas concessions. His practice is also significant in the area of loan and bond finance and in the field of capital markets, having advised on several securitisation transactions (including the first securitisation transaction under the new law and the first synthetic securitisation) and covered bonds issuances, and having worked on several IPOs of state-owned companies.

Vera Esteves Cardoso
Tel: +351 213 817 400 / Email: vcardoso@mlgts.pt

Vera Esteves Cardoso joined Morais Leitão in February 2023 as a consultant in the banking and finance team. She began her professional career at Banco de Portugal (the Portuguese Central Bank) in the anti-money laundering and counter-terrorist financing supervision division, having coordinated the market entry team over the last few years, gaining specific experience in the field of authorisations for acquisitions and increases of qualifying holdings, licensing, passporting and registration and ongoing supervision of crypto-asset service providers (which this team was fully responsible for).

At Banco de Portugal, Vera participated actively in Portugal FinLab, the Portuguese innovation hub for fintechs, and in the development of European guidelines on authorisations, including in what concerns licensing under PSD2, as well as in focus groups related to stablecoins and Technological Free Zones.

Currently, Vera develops her work primarily in banking law, fintech, and crypto-asset service providers, with a special focus on market entry and compliance matters.

Ashick Remetula
Tel: +351 213 817 400 / Email: aremetula@mlgts.pt

Ashick Remetula joined the firm in 2023. He is a member of the banking and finance department, as well as a member of Team Genesis.

Ashick has experience in fintech, finance and venture capital/private equity, both on the side of investors and startups, and also in projects in the energy and natural resources sector, including M&A transactions.

Ashick develops his practice in the fintech area with emphasis on companies dealing with new and emerging technologies, matters related to blockchain, crypto and web3.0, essentially in the context of attracting and making investments, licensing and regulation. Moreover, Ashick also advises those companies in project management issues from a legal standpoint.

Ashick also engages in advisory in projects managed by Fintech House and Nova SBE's innovation ecosystem.

Morais Leitão, Galvão Teles, Soares da Silva & Associados

Rua Castilho, 165, 1070-050 Lisbon, Portugal
Tel: +351 213 817 400 / URL: www.mlgts.pt

Romania

Sergiu-Traian Vasilescu, Luca Dejan & Bogdan Rotaru, VD Law Group
Flavius Jakubowicz, JASILL Accounting & Business

Government attitude and definition

From a social point of view, in Romania, cryptocurrencies and blockchain have experienced a structured evolution in three stages: innovation (genesis); phenomenon ("FOMO", or fear of missing out); and social reality. After initially appearing as an innovation and quickly becoming a social phenomenon, they now represent a social reality that is impossible to dispute (they exist, and they are valuable).

Despite retaliation and lack of regulation, the technological evolution could not be stopped, and the new emerging technologies quickly became a means of investment, a conventional payment method, a decentralised alternative to the financial banking system, a scalable solution to various social problems and even a mechanism for marketing and promotion.

These new emerging technologies have simultaneously succeeded in both innovating through native functionality and transforming traditional industries. Furthermore, we have witnessed the creation of a whole new industry based on distributed ledger technology ("DLT"), which has proven capable of providing innovative solutions that have forced traditional industries to find solutions to integrate these technologies.

When it comes to the supervision and regulation of personal and professional activities related to blockchain and cryptocurrencies, Romania continues to take promising steps. In particular, the Romanian Government tends to have a positive attitude towards their potential benefits, as demonstrated by its attempts to understand the workflows and refraining from blanket bans on activities related to this industry.

It should be noted that the Romanian legislative body, as far as the regulation of blockchain and cryptocurrencies is concerned, mainly follows the legal regime and guidelines issued by the EU. Therefore, our analysis will focus first on the relevant direction taken by the EU, as well as the implicit or explicit adherence of the Romanian Government to this acquis, and then outline the elements that can be considered specific to the national position.

Although the blockchain-based Web3 space witnessed significant disturbances throughout 2022–2023 caused by the collapse of several massive projects, it also benefitted from major new applications and research intended to increase the value and confidence placed in the industry. These developments, which clearly show that the market is maturing, could not have been overlooked by the legislators in charge, who should be congratulated for recording the busiest year to date in terms of the adoption of important cryptoasset-related legislation (i.e., the Digital Operational Resilience Act, the regulation on a pilot regime for DLT-based market infrastructures ("DLT Pilot Regime"), the Markets in Crypto-Assets ("MiCA") Regulation, etc.). Most importantly, when looking at the recent legislative changes, regardless of the overall level of implementation, the outlook of officials in relation to cryptoassets can be considered favourable, as discussed in more detail below.

Romania contributes to the InvestEU Programme, and implicitly to the Strategic Technologies for Europe Platform, which continues to support the EU's position as a world-recognised pioneer, *inter alia*, in the field of blockchain technology. Romania also adhered to the Digital Decade 2030 policy programme, thus being added to the list of multi-country projects that aim to take advantage of future blockchain-based applications.

As stated when implementing Horizon Europe, "[*a*] *new global wave of breakthrough innovation is coming, one that will be based on more 'deep-tech' technologies such as block-chain* […]. *Europe must ride that wave* […]".[1] Accordingly, the European High Performance Computing Joint Undertaking, of which Romania is a member, provides that "*the Union should provide an opportunity for its supply industry to leverage on* […] *large-scale and emerging application fields such as* […] *blockchain technologies*".[2]

At the same time, the Romanian Government's efforts aim to tackle climate change and environmental protection in a comprehensive way by exploring the benefits of blockchain technology, as envisioned by the EU Green Deal.[3]

Adequate national and European funding will therefore be made available to actors involved in experimental development and industrial research related to Web3. Activities of this type will be encouraged and supported in Romania, especially since they are seen as an alternative means of financing small and medium-sized enterprises ("SMEs"), as well as providing additional opportunities to consumers, and as key elements of future financial services.

Moreover, while blockchain innovations have been granted with a 100% coefficient of financial aid in accordance with the Recovery and Resilience Facility, Romania looks forward to operationalising important official pilot programmes such as the European NFT Platform, a space for the Metaverse or the embedded supervision of decentralised financial institutions and activities.

We may also assert that it is expected for Romania to be significantly involved in the EU Blockchain Observatory and Forum, as well in the Connecting Europe Facility, and thus to expand its relevant institutions' knowledge of the cryptocurrency market within an inclusive paradigm.

As regards the measures taken by the Romanian Government in the field of cryptocurrency, we firstly refer to the specific programmes for 2021–2026 for the financing of perfection and requalification of employees, as well as the digitalisation of SMEs. It is worth noting that, in Romania, the professions of blockchain architect and developer were officially recognised as early as 2011.

The Romanian legislature has expressed reservations in 2018 about funding other centres for blockchain research, citing a disproportionate burden on the budget. Nevertheless, the rapid adoption of cryptoassets (there are now more than 2 million crypto holders registered in Romania, or 10% of the population) has led the National Bank of Romania to create and host a Fintech Innovation Hub, and since 2022, a specialised department has been established within the Ministry of the Interior to support initiatives related to the use of new technologies and digital solutions, including blockchain.

Furthermore, as promised by the current Government as part of its 2023–2024 Executive Programme, accelerating digital transformation is the benchmark for defining Romania's new development model. Blockchain, in particular, is intended to occupy a central position among the technologies that are considered as such.

As a relevant example of this approach, the first public project related to these new emerging technologies was announced in Q3 2022 by the National Post Office, which plans to launch a collection of non-fungible token ("NFT") stamps to commemorate its 160th anniversary.

On a different note, not all elements of the cryptocurrency industry are seen as offering both disruptive and unharmful uses of technology. As a result, the Romanian Government has set out to prevent the malicious practices that could be associated with these advanced digital novelties, such as money laundering, organised crime or, more recently, the circumvention of war-related economic sanctions imposed against Russia.

The Romanian Government first decided to secure the national interest by regulating such new emerging technologies in the most sensitive areas, including from the tax, anti-money laundering/know-your-customer ("AML/KYC") and criminal law perspectives.

In this context, the Romanian Government has adopted Emergency Ordinance ("GEO") No. 111/2020 in view of completing and amending Law No. 129/2019 for preventing and combatting money laundering and terrorist financing. The purpose of the GEO is to strengthen crypto regulation in Romania in view of AML policies (please see "Money transmission laws and anti-money laundering requirements" below).

According to the GEO, the provision of crypto-to-fiat exchange, as well as digital wallet services, should be subject to authorisation and/or registration by the Commission for the authorisation of foreign exchange activity within the Ministry of Public Finance as well as obtaining technical approval from the Romanian Digitization Authority. Although a draft decision was published by the Government in May 2022, at the time of writing, the provisions regulating the activities of providers of exchange services between virtual and fiduciary currencies and providers of digital wallets are still not fully enforceable due to the lack of adoption of implementing regulations.

However, if and when this government decision becomes applicable, providers of virtual currency exchange services and digital wallet services already operating in the European markets and fulfilling the requirements of the fifth Anti-Money Laundering Directive ("AMLD5") will not be exempted from the Romanian authorisation procedure if they intend to expand their activity in this country. Thus, in order to operate legally in Romania, all such providers will be required to obtain a licence from the Romanian Digitization Authority.

Cryptocurrencies are not considered legal tender either in Romania or at the EU level. The EU envisions the issuance of a digital Euro but states that it should not be seen as a proper cryptocurrency. Nevertheless, pursuant to the MiCA Regulation, which will be directly applicable in Romania and is supported by the Romanian legislator, stablecoins can be seen as equivalent to electronic money.[4]

Cryptocurrency regulation

Essentially, the relationship between blockchain and cryptocurrencies should be seen as a whole-part relationship (blockchain representing the innovation, and cryptocurrencies standing as just one of the applications of DLT) and the two notions are therefore worth analysing together: blockchain being "the vehicle" and crypto its "nuclear engine" to success. Therefore, while cryptocurrencies could not exist without blockchain, the latter could have not become the subject of our analysis without the notoriety acquired by cryptocurrencies. Thus, our analysis will cover both as a whole and touch upon the specific particularities of each of them.

In our opinion, regulating a technology can block its development and directly limit developers' innovation. Unfortunately, strict regulations may lead to existing and future use cases or blockchain infrastructures that have not been discovered being classified as illegal or non-compliant products.

It should also be noted that cryptocurrencies are not prohibited in Romania, nor are they prohibited in any particular way. Given that the national legal framework is aligned with the EU Digital Finance Package (for the reasons explained in "Government attitude and definition" above), at least until the legal acts comprising it enter into force, Romania can be considered to lack a fully enforceable regulation of crypto-related activities.

In the meantime, specialised practitioners (lawyers, accountants, tax consultants, and experts) have been forced to identify similar concepts in the national legislation and to adapt traditional institutions to these new technologies.

In this context, it is worth assessing the state's concern about the extent to which the decentralisation of key activities (e.g., financial and banking operations) threatens the Government's control, which could lead to the enactment of repressive regulation towards centralisation (for example, a ban on using exchanges or wallet providers that are not authorised or do not carry out AML/KYC verifications is still at the project stage at government level).

However, the Web3 market raises completely different organisational principles and therefore complex issues for the regulator, with specific characteristics related to elements such as: (i) technical means of deployment; (ii) storage; (iii) testing; (iv) restriction; (v) traceability; (vi) governance; (vii) reversibility; (viii) originality; (ix) identity; or (x) monitoring. As stated by SEC Commissioner Caroline Crenshaw, issues of lack of transparency, pseudo-anonymity and compliance with fundamental market rules in the decentralised finance space are driving unprecedented complexity in the legislative process.

Apart from the EU acquis, Romania has nevertheless managed to adopt isolated provisions in its national legislation in the following key areas:

- fiscal aspects applicable exclusively to individuals, such as taxation of income generated by individuals from crypto-related activities;
- security aspects regarding the prevention of money laundering and combatting the financing of terrorism, namely a series of rules and restrictions applicable to the providers of exchange services (exchanges) and cryptocurrency storage service providers (wallets). Even though such regulation has already been enacted in Romania, it is not currently in force due to the lack of secondary legislation – the adoption of which suspends the primary legislation's effects by 12 months; and
- aspects in connection with criminal law, i.e.: (i) qualification of digital currencies as non-cash payment instruments; (ii) extending the scope of criminalisation of certain offences to include crypto-related activities; and (iii) criminalising the possession of cryptocurrencies resulting from criminal offences.

Conversely, the lack of explicit regulation so far would point to a number of important features that these new emerging technologies offer and that have not yet been thoroughly explored in Romania, such as: (i) security token offerings; (ii) tokenisation (either full or fragmented) of valuable goods (real estate, art, precious metals and diamonds industry); (iii) payment processing and lending (financial banking industry); or (iv) administration of cryptocurrencies (brokerage and asset management industry).

Transactions with virtual currencies (cryptocurrencies) were regulated for the first time in 2019 under Law No. 30/2019, which introduced provisions in the Romanian Tax Code regarding the taxation of income thus obtained. Also, since 2019, the Romanian Criminal Code has classified digital currencies as a "means of payment without cash". The only purpose of this latter classification is to sanction crimes such as theft or embezzlement committed in connection with cryptocurrencies.

We may also assert that there are voices within the crypto space, referred to as "veterans", including individuals, legal entities and associative companies, who are calling for a more permissive regulation of the activity as a whole and more energetic public solutions to the outstanding problems (e.g., the fight against fraud, and the adoption by central banks of coherent supporting policies aimed at creating a link between cryptocurrencies and traditional currencies).

It is interesting to note that the lack of a dedicated regulatory framework in Romania has so far not been a major drawback for entrepreneurs running companies that deal with cryptoassets. In addition, major legislation, which will come into force in Q4 2023 and 2024, is expected to promote a level playing field for innovation, growth and competitiveness, both in the European single market and globally.

Also, according to the National Bank of Romania, the manifestation of risks specific to the holding and trading of virtual currencies and the significant price volatility of some traded virtual currencies do not currently pose a threat to financial stability in Romania.

Sales regulation

Buying and selling crypto

At the time of writing, buying, holding and selling Bitcoin or any other token generally referred to as a utility token is not restricted in Romania. As with any purchase of commodities, AML/KYC and tax rules must be complied with.

However, issuing, buying, storing, or selling security cryptocurrencies are regulated by means of Law No. 126/2018 on financial instruments markets and Law No. 24/2017 on issuers of financial instruments and market operations, which transpose the EU's second Markets in Financial Instruments Directive ("MiFID II"). As such legislation was not originally designed with the specificities of the Web3 market in mind, the DLT Pilot Regime became applicable on 23 March 2023.[5] Cryptoassets that fall within the scope of the latter regulation must be traded separately from cryptoassets that will be subject to the MiCA Regulation, while exemptions from MiFID II may apply on a case-by-case basis.

With regard to business tax, legal entities may also acquire Bitcoin or utility tokens, *inter alia*, if these are the subject of their current activity (e.g., exchanges, traders, investment vehicles) or if such digital assets are necessary for the performance of their current activity (e.g., making or accepting payments in crypto, accessing a service or purchasing a product that can be purchased with a specific token/crypto). Any acquisition that is not necessary for the conduct of the business will be construed as non-deductible spending, hence it may be requalified as a personal benefit offered to shareholders or employees in the form of dividends or salary. In this case, the company at hand may be required to collect and pay the corresponding taxes.

Buying and selling with crypto

Crypto payments are being increasingly accepted by major retailers, either directly or through payment gateways to avoid technical implementation, transaction and wallet management issues.

Under the existing legal institutions, cryptoassets are generally qualified as intangible assets. From a technical point of view, a payment in crypto represents an exchange, not a sale agreement, and although no cryptocurrency is considered legal tender, parties may voluntarily accept crypto as an alternative means of payment.

A set of new tax systems, accounting rules and guidelines are being developed by professional organisations as preliminary instructions for the anticipated legislation. In particular, these preparations are meant to aid the constantly increasing number of online stores that accept Bitcoin or other cryptocurrencies, thus creating a safe climate for the shopping experiences of the future.

Taxation

Taxation and accounting, in the context of ongoing technological progress, remain advanced discussion topics, causing uncertainty and debates regarding the optimal approaches, even in well-established sectors. According to Romanian legislation, it is assumed that any benefit, whether in physical or digital form (traditional currency, cryptocurrency, services, or commodities like gold or silver), is subject to a tax regime specific to the income category of the taxpayer. Like other industries, revenues from emerging technologies are also taxed in Romania.

Therefore, taxpayers have the responsibility to declare and pay taxes in accordance with the current regulations. Factors such as the nature of the activity (for example, trading *versus* selling NFTs), the legal structure under which they operate (individual, LLC, sole proprietorship) and the volume of income influence the taxation regime. It is essential to understand that the same operation can have different tax implications depending on individual specifics. In the context of cryptocurrency volatility or large transactions from initial coin offerings ("ICOs"), it is vital to understand the financial dynamics of the business to determine when revenues become taxable. Receiving cryptocurrency as payment for services or goods translates into a revenue-generating activity that must be declared and taxed.

As of 2021, the global shift towards digital economies, driven partly by the COVID-19 pandemic, has amplified the urgency for countries to adapt their taxation and accounting regulations. Digital assets like NFTs and cryptocurrencies are no longer peripheral financial instruments but have started to gain mainstream acceptance. Various countries have been adjusting their regulations to ensure fair tax collection without hindering innovation.

In practice, we have identified major confusion regarding the moment from which fees and taxes are due, namely the approach that tax is due only at the moment when cryptocurrencies are converted into fiat currency. Such outcome is partially valid, and is lawful only if the activity (i) is carried out by an individual, (ii) consists of the trading of cryptocurrencies ("trading"), and (iii) involves an economic cycle that ends with the conversion of crypto-currencies into fiat currency.

Therefore, in order to determine the proper manner for the taxation of income obtained by individuals from activities that include cryptocurrencies, it is compulsory to determine and acknowledge the economic cycles related to each technical operation. As a general rule, the taxpayer has the obligation to pay tax on the income obtained from cryptocurrencies, namely if the patrimony has increased, regardless of the method (e.g., the person has acquired/received several cryptocurrencies having a higher value than one originally invested or his amount of fiat currency has increased).

Therefore, with respect to trading activity carried out by individuals, taxes and fees are due at the completion of such activity, which often (but not always) overlaps with the exchange of cryptocurrencies into fiat currency. The principle of taxation specifically applies to the value increase obtained following the completion of an activity cycle and does not refer exclusively to conversion into fiat currency.

However, we will consider a completed cycle and therefore the obligation to pay the tax due if, for example, during a six-month period, a person multiplying the number of cryptocurrencies held decided to definitively cease trading activity or decided to buy NFTs with the funds obtained from such activity, without transforming them into fiat.

For the purpose of understanding the scenario whereby an individual is required to pay taxes even if the income obtained is in cryptocurrency and has not been converted into fiat currency, we will assess the example of an individual creating and selling an NFT in exchange for a determined amount of Tether ("USDT") and subsequently using such funds to acquire tokens to be allocated to the staking process. In this case, we identify two distinct economic cycles generating income; namely, the sale of the NFT and the staking reward. Therefore, the individual will owe tax for the equivalent in Romanian currency ("RON") of the amount of USDT received for the sale of the NFT and subsequently for the equivalent in RON of the amount of tokens received as a reward from the staking activity.

Furthermore, we consider it worthwhile to assess the case of an individual obtaining cryptocurrencies as a result of the activity of validation ("staking") by reference to obtaining tokens as a result of a release activity ("airdrop").

Unlike trading activity, staking or token release activities (airdrop) may be construed as completed at the moment when the taxpayer receives the cryptocurrencies and the obligation to pay the relevant taxes is therefore due.

However, even in this situation, it may be difficult to precisely determine the moment of increase of the taxpayer's patrimony. Clearly, in cases whereby cryptocurrencies are received in the taxpayer's digital wallet, the patrimony increases with the value of the cryptocurrencies received, with the obligation to pay the taxes due according to the applicable tax regime.

Furthermore, a distinct analysis arises in the context where the taxpayer is only entitled to receive cryptocurrencies and in turn has the possibility to claim them without effectively doing so. Likewise, debatable approaches also arise in the case of systems that allow options for automated direct allocation of generated cryptocurrencies, without receiving them in the wallet ("compound"). In such case, the applicable tax regime is determined by reference to the income-generating mechanism following an in-depth analysis of the smart contract's technical infrastructure.

In addition to the foregoing general principles that are applicable accordingly with respect to legal entities, it is important to establish the exact context and technical manner in which revenues are generated.

As mentioned, the Romanian Tax Code only provides trading activity performed by individuals, establishing that taxes are due by individuals at the moment of converting cryptoassets into fiat. Unfortunately, many crypto holders apply this taxation mechanism to all crypto-related revenues, despite the method ("economic cycle") by which the cryptoassets were obtained and/or generated, such as cryptoassets received as a means of payment for selling a house.

However, there are also scenarios in which trading platforms allow the holding of a wallet in fiat. In such cases, the gain will be deemed to be realised after the transfer made to the wallet available in fiat and must be declared, regardless of whether it is further transferred to the bank account or used to perform other transactions on the platform.

Considering all the above-mentioned information regarding taxable income resulting from crypto-related activities, individuals are bound to declare such earnings by filing the financial statement for natural persons, also known as the "Sole Statement".

The Sole Statement is a smart PDF in which individuals self-declare the equivalent in national currency of the entire income generated from crypto-related activities, without providing any other information regarding how the cryptoassets were generated. However, additional information regarding all the revenues obtained may be required by the tax authorities, especially when a more than 10% ratio between the expenses and self-declared income is noticed.

It is worth noting that there exists a financial threshold that governs the taxability of these transactions. Specifically, revenues less than RON 200 (approximately EUR 40) for each transaction are exempt from taxation, but with the stipulation that the cumulative annual income must not breach the cap of RON 600 (equivalent to around EUR 120). Additionally, should the aggregate profits derived from alternative revenue streams coincide with or surpass 24 times the gross minimum wage (an estimated EUR 11,000), the taxpayer would incur an additional health insurance contribution, which would amount to around EUR 1,100.

On the other hand, corporate income is subject to the standard income tax applicable to all companies having fiscal residency in Romania. In the case of a small business or microenterprise, the profits will be taxed at a standard flat rate of 1% provided the business maintains at least one full-time employee, together with a dividend tax in the amount of 8% and any applicable social security contributions. A company should be very diligent in maintaining an accurate and proper record of all taxable cryptocurrency transactions (receiving payments in cryptocurrencies, exchanging, etc.).

In conclusion, it is crucial to stay updated on upcoming changes in fiscal policies. As we move past 1 January 2024, predictions indicate significant modifications to the overall fiscal framework. This underscores the continuous need for those involved in the cryptocurrency sector to remain vigilant and adaptable.

Money transmission laws and anti-money laundering requirements

At the time of writing, AMLD5 is applicable, which addresses the need to implement legislative measures in order to reduce the risks stemming from the anonymity of transactions performed with virtual currencies. Romania has enacted GEO No. 111/2020, laying down rules on entities involved in cryptocurrency transactions that are thus bound to identify and report suspicious transactions that may breach any provision concerning the AML framework.

GEO No. 111/2020 most notably extends the concept of reporting entities and their scope. It also introduces the obligation to apply standard KYC measures based on a secure identification process.

Pursuant to GEO No. 111/2020, authorised entities (e.g., digital wallet providers, credit institutions, final institutions, gambling service providers, auditors and certified public accountants) become reporting entities in accordance with the AML legislation and have the obligation to report suspect transactions to the National Office for Preventing and Combating Money Laundering. All these provisions and rules are meant to provide effective protection for the beneficiaries of such types of services, as well as for the providers thereof against scams and fraud.

Under the current legal regime, the Romanian Government has planned to issue specific legislation for the authorisation of crypto-to-fiat exchanges and digital wallet providers, as discussed in "Government attitude and definition" above.

On a separate note, after three years of rumours that the National Bank of Romania was unofficially banning cryptocurrencies, it has dismissed all such rumours through a press release. However, it has expressed that the current national and European regulations

will allow commercial banks to work with cryptocurrency exchanges and digital wallet providers, provided they apply KYC and risk management measures in the area of AML and terrorist financing.

Furthermore, the Romanian Senate has expressed its official position towards the Proposal for a Regulation of the European Parliament and of the Council on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing, by stating that it is in line with the latest amendments of the Financial Action Task Force in the sense of including cryptoasset service providers.

The AML legal framework is expected to be updated during 2024, with the adoption of a new AML Directive and subsequent legislation (AMLD6). In particular, this will create more tailored rules in relation to cryptocurrency exchanges and custodians of cryptoassets and will also provide clearer definitions of offences assimilated to money laundering in the context of cyber and environmental crime.

Promotion and testing

In Romania, there is no prohibition on the promoting or advertising of buying or using services related to Bitcoin or any other utility cryptoasset. All regulations related to fair marketing advertisement and consumer protection are applicable to all business industries irrespective of their activity.

However, the advertising of services related to gambling, securities or investments is subject to prior endorsement issued by competent authorities, and there are instances when they may be completely forbidden. Romania has not implemented any sandbox or similar testing programmes in relation to these new emerging technologies.

A Fintech Innovation Hub is currently operational under the coordination of the National Bank of Romania. There are several other private initiatives and partnerships that may involve public support for the development of blockchain applications, and Romania has introduced financial incentives for companies active in this field.

At the EU level, the Commission introduced a so-called European Blockchain Regulatory Sandbox on 14 February 2023, which establishes a pan-European framework for regulatory dialogues to increase legal certainty for innovative blockchain solutions. Furthermore, at the end of Q1 2023, the EU DLT Pilot Regime entered into force, which applies to tokens that represent financial instruments. This legislative act creates a *sui generis* sandbox regulation based on which the relevant EU authorities, including the European Commission, shall draw periodic conclusions for further amendment of the dedicated legal framework.

More than 15 new activities based on new emerging technologies have also been established by private service providers in Romania, including: (i) ICOs; (ii) initial exchange offerings; (iii) cryptocurrencies that have 1:1 parity with fiduciary coins (stablecoins); (iv) exchange services between cryptocurrencies (crypto exchanges); (v) exchange services between cryptocurrencies and fiat currency; (vi) cryptocurrency storage services (crypto wallets); (vii) services for monitoring transactions/payments with cryptocurrencies (tracking tools); (viii) transaction validation activities (mining farms); (ix) liquidity assurance services (farming pools/landing platforms); (x) e-commerce services (marketplace); (xi) cryptocurrency payment/receipt services (transaction/payment processors); (xii) online games (crypto games); (xiii) NFT generation services; (xiv) secure telecommunications services; and (xv) governance system decentralisation services.

Traditional industries have not remained passive, either, and have begun to adapt their activities in such a way as to integrate the functionalities of the new emerging technologies for: (i) accepting payments in cryptocurrencies (retail and automobile industries); (ii) organising databases to create transparency and immutability (IT industry); (iii) cryptocurrency fundraising and democratisation of investments (small amounts from a large number of investors – crowdfunding industry and private investments); and (iv) using surplus energy to validate transactions in the blockchain (mining – the green energy industry).

Ownership and licensing requirements

Taking into account that Romania does not have a specific enforceable regulation dedicated to blockchain-based activities, all crypto owners or service providers are obliged to comply with the general trade rules and, therefore, the obligation to implement additional due diligence to prevent and combat money laundering and terrorist financing. However, there is no restriction on holding or owning Bitcoin or any other utility token.

However, the implementation of activities related to these emerging technologies (mining, farming, validation, staking, exchange, custodian services, etc.) requires a thorough analysis for identifying the correlative obligations. Therefore, although an activity may be physically performed by using the blockchain technology, from a legal perspective, such activity may only be carried out (i) by a certain category of economic operators (card payments, loans, credits, lotto), (ii) after authorisation or licensing (gambling), or (iii) after complying with certain procedures (KYC/AML/PEP check).

In practice, the applicability or purpose of using such technologies can be qualified into four categories, each with a different legal and economic regime:

a. non-continuous activity (rendered for personal purpose without recurrence), referring to activities carried out (usually) as an individual, which should generate income that may not be qualified as the main source of income;
b. continuous activities (for business purposes), which involves carrying out a recurring activity that represents the main source of income, usually as an individual;
c. activities carried out by professionals when providing services for third parties (e.g., trading services or technological support services); and
d. activities performed solely for marketing and promotional purposes.

Considering the foregoing classification, it may be determined whether a specific activity may be duly performed as an individual or must observe the regulation applicable to legal entities. As per Romanian regulation, recurring trade activities or activities that are performed for professional purposes may only be performed by a legal entity (e.g., limited liability company, joint-stock company, authorised legal person) under a determined NACE code.

Mining

Even though no directly applicable legislation has been enacted, it may be strongly argued that mining Bitcoin or other cryptocurrencies is not forbidden in Romania, as any gains stemming from such activities are subject to taxation in accordance with specific provisions under the Romanian Tax Code.

Last year, over 10,000 individuals and legal entities were estimated to perform crypto-mining activities in Romania, and an important exchange platform is proposing to issue "mining certificates".

Conversely, for a full representation of crypto-mining activity in Romania, we encourage you to look at the Helium miners map (available at https://explorer.helium.com) and take into account that there are at least 100 times more Bitcoin and Ethereum miners than Helium.

Fortunately, the Romanian authorities have taken into account the current issues concerning crypto-related activities and, consequently, the need to adapt national legislation to a rapidly evolving economic environment. Moreover, it can be argued that the relevant legal framework should become more business-friendly in the future, while also considering the environmental impact and specific objectives in this regard.

Border restrictions and declaration

Unlike other jurisdictions, under Romanian regulation, natural persons are not bound to declare the crypto holding or assets expected to be obtained in the following year. However, as stated in the foregoing sections, individuals gaining income from cryptocurrencies (NFTs included) must declare such gains as "income from cryptocurrencies" under the unique financial statement for natural persons. Such statement must be submitted to the tax authorities by 25 May of the year following the year in which the income was generated.

Furthermore, a natural person's cryptocurrency gain for tax purposes shall be determined as the positive difference between the selling price and the purchase price, by observing any deductible direct costs related to the transaction (e.g., bank fees, exchange trading platform fees). Please note that any acquisition of goods or services based on cryptoassets or with a crypto card (such as a Binance card) shall be construed as an "exit" and the same fiscal regime will thus become applicable.

Given that majority of crypto acquisitions were made between 2015 and 2017, many holders are unable to prove the value of the acquisition in question; therefore, the income generated is usually determined by reference to the amount of fiat received in the bank account, plus the fiat equivalent of the services or goods acquired directly with crypto or using the crypto (Binance) card.

Legal entities must keep audit accounts and declare their holdings (like any other assets) on a monthly, quarterly or annual basis, based on the applicable inventory and tax regime, simply by filling in the relevant accounting forms. Failure to comply with such requirements can be construed as tax evasion.

Reporting requirements

According to GEO No. 111/2020, reporting authorities are bound to submit to the Office for Preventing and Combating Money Laundering any transaction exceeding the threshold of EUR 10,000 or transactions that cumulatively exceed such value.

The reporting authorities listed in the "Money transmission laws and anti-money laundering requirements" section above are required to increase the degree and nature of monitoring of the business relationship in order to determine whether such transactions or activities are suspicious. According to the regulations in force, the authorities are bound to report suspicious transactions exclusively to the Office if they acknowledge, suspect or have reasonable grounds to suspect that the assets are subject to criminal offences or are related to terrorist financing.

In a such case, the reporting authorities must immediately submit a suspicious transaction report to the Office before any customer transaction relating to the reported suspicion is carried out. The suspicious transaction will not be authorised until 24 hours after the Office has registered the report. If the Office does not order the suspension of the transaction within the aforementioned period, the reporting authority may carry out the transaction.

In order to evaluate the transaction and conduct the due verifications, the Office may suspend a transaction for up to 48 hours, as a result of information received pursuant to the provisions of the law, as a result of requests from Romanian judicial bodies or foreign institutions with similar functions, or on the basis of other information in its possession.

If the reported suspicion is not confirmed, the Office must decide to end the suspension of the transaction within 48 hours. The decision shall be notified to the reporting entity without delay and shall be implemented immediately.

Estate planning and testamentary succession

In the absence of any specific regulation to date, Bitcoin and any other cryptoasset are subject to the regime applicable to any other valuable patrimonial asset that a person may own and transfer to another person either during or after his lifetime. Therefore, all cryptoassets are passed on to heirs (either by virtue of law or by virtue of will) in the same way as any other asset.

In recent years, centralised service providers have started to implement internal procedures for transferring the assets held in a user's account to the entitled relatives or persons, as previously carried out by banks, brokers or custodians (vaults).

Unfortunately, in the case of decentralised systems (private wallets) where only the owner knows the private key that allows access to the assets, funds are considered lost forever without a backup plan.

However, even in the case of centralised platforms, if there is no specific request from the entitled persons or no emergency contact if the account has been used for a certain period of time, the funds will remain in the custody of the platform forever, much like the funds of those who died in the First and Second World Wars, which are still held in Swiss private banks.

* * *

Endnotes

1. https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32021D0764
2. https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32021R1173
3. Moreover, as asserted through the last EU budgetary policy, "*there is a need to strengthen the links between these communities and policy makers (at Union, national and regional levels), given the strong contribution such innovations can make to key policy priorities such as climate change*", https://publications.europa.eu/resource/cellar/3a6f2e59-b34a-11ed-8912-01aa75ed71a1.0006.03/DOC_1
4. https://www.ecb.europa.eu/ecb/educational/explainers/html/digital_euro_central_bank_money.ro.html
5. Regulation (EU) No. 2022/858 of the European Parliament and of the Council of 30 May 2022 on a pilot regime for market infrastructures based on distributed ledger technology, and amending Regulations (EU) No. 600/2014 and (EU) No. 909/2014 and Directive 2014/65/EU (Text with EEA relevance).

* * *

Acknowledgment

The authors would like to thank Eduardo Neamtu for his contribution to this chapter. Eduardo is a Senior Associate at VD Law Group. A graduate of the University of Bucharest,

Eduardo has since gained extensive experience in the legal field, with a focus on high-level arbitration, dispute resolution, real estate and corporate law cases, in which he has achieved outstanding victories.

Eduardo has a passionate focus on the emerging tech and fintech industries and a drive to provide innovative legal solutions for complex transactions. His ability to easily analyse, combine and synthesise large amounts of information from different areas of law is constantly demonstrated and enhanced.

Eduardo is leading the way in the development of a whole range of beneficial use cases for blockchain and cryptocurrencies, their proper in-depth regulation and their understanding by a growing audience.

Sergiu-Traian Vasilescu
Tel: +40 753 036 360 / Email: sergiu.vasilescu@vdlawgroup.com

Sergiu-Traian Vasilescu is the founder and Managing Partner of VD Law Group, advising clients with IT&C projects in areas such as tech, fintech, e-commerce, digital media, blockchain, cryptocurrency, privacy and data protection.

Educated in an entrepreneurial spirit at Université Paris 1 Panthéon-Sorbonne, Sergiu is strongly skilled in anticipating potential cross-disciplinary risks and regulatory and technical issues.

Moreover, Sergiu has gained extensive experience in private investments, pharmaceuticals and medical-related legal issues.

Luca Dejan
Tel: +40 723 066 026 / Email: luca.dejan@vdlawgroup.com

Luca Dejan is the founder and Partner of VD Law Group advising clients in private investments, finance, corporate transactions and real estate. Luca has also gained substantial experience in dispute resolution, assisting clients in highly sophisticated and technical litigation files such as FIDIC, public procurement, commercial, construction and real estate and medical malpractice disputes.

Combining a strong academic background and practical knowledge gained in one of the most reputable legal teams, Luca has significant experience in advising high-level clients in landmark projects for the Romanian business market. He is committed to producing outstanding results in every project.

Flavius Jakubowicz
Tel: +40 372 285 720 / Email: flavius@jasill.ro

Flavius Valentin Jakubowicz has over 15 years of experience in financial analysis and consulting, accounting, tax, audit and due diligence processes and as a forensic expert, and in the last four years has become a tax specialist in the world of crypto and blockchain technology.

As Managing Partner of JASILL and one of the most experienced Romanian providers of integrated accounting, tax, legal and business consulting services, he coordinated the tax consulting, accounting and reorganisation services teams, as well as multidisciplinary teams with financial, tax and legal experience in due diligence projects.

Bogdan Rotaru
Tel: +40 729 817 623 / Email: bogdan.rotaru@vdlawgroup.com

Bogdan Rotaru, Partner at VD Law Group, brings a wealth of knowledge and experience to the firm. With a background rooted in dispute resolution and corporate – M&A, Bogdan has established a broad spectrum of expertise that extends to the fields of pharma, intellectual property, IT&C, and data privacy. He was educated at the University of Bucharest Law School and honed his skills as an attorney-at-law at one of Romania's leading law firms. In addition to his private practice, Bogdan has also gained invaluable insights through his in-house legal work for a worldwide corporation.

VD Law Group | JASILL Accounting & Business

291–293 Splaiul Independentei, Riverside Tower, 13th floor, District 6, Bucharest, Romania
Tel: +40 753 036 360 / URL: www.vdlawgroup.com
Tel: +40 372 285 720 / URL: www.jasill.com

Singapore

Kenneth Pereire & Lin YingXin
KGP Legal LLC

Government attitude and definition

The Singapore Government takes a pragmatic, cautious and tailored approach toward dealing with cryptocurrencies. While the Government recognises the economic and social potential of cryptocurrency and seeks to foster a conducive regulatory environment for its adoption within Singapore's financial landscape, at the same time, the Government is exercising caution by seeking to identify the risks involved, for example, in terms of consumer protection and anti-money laundering/counter-financing of terrorism, and then to manage these risks in a proportionate manner including through licensing (where applicable).

Cryptocurrencies are not being treated as the equivalent of money in Singapore. Depending on the characteristics of each cryptocurrency, it may be treated as a regulated product such as a capital markets product (including securities), e-money, or a digital payment token ("**DPT**"), or else as an unregulated digital token that is strictly used for utility purposes.

The Monetary Authority of Singapore ("**MAS**"), which is Singapore's central bank, has not issued or backed any cryptocurrencies for retail use. However, it has partnered with participants in the industry to conduct a collaborative project, "Project Ubin", to explore the use of blockchain and distributed ledger technology for the clearing and settlement of payments and securities. The payments network prototype that was developed through this project would facilitate the development of a cross-border payments infrastructure, as well as customer applications. "Project Dunbar", a project by the Bank for International Settlements Innovation Hub and central banks including MAS, which was announced on 22 March 2022 to have been completed, was said to have demonstrated that central bank digital currencies ("**CBDCs**") could be used by financial institutions to transact directly with each other through a common platform. This potentially reduces the need for intermediaries, as well as the costs and time required for the processing or cross-border transactions.

On 3 November 2022, MAS launched Ubin+, which is a collaboration with international partners on using wholesale CBDC for cross-border foreign exchange settlement.

MAS has also embarked on "Project Orchid", which seeks to establish the technical infrastructure for the building of a retail CBDC system. Nonetheless, MAS has been focusing more on wholesale instead of retail CBDCs because the issue of financial inclusion is not an urgent one in Singapore.

MAS is testing the potential of asset tokenisation across additional categories of financial assets such as digital structured products, tokenised investment vehicles, tokenised asset-backed securities, tokenised bonds, and tokenised bank liabilities, through industry pilots in collaboration with financial institutions, under the recently expanded "Project Guardian". This could contribute to improving liquidity and inclusivity in the financial markets, while increasing the efficiency, affordability and accessibility of financial services.

The Government has issued cryptocurrency trading guidelines, passed amendments to the Payment Services Act 2019 ("**PSA**"), and passed the Financial Services and Markets ("**FSM**") Act, to address additional risks, including those to retail investors and money laundering.

As for judicial developments, it is notable that the Singapore High Court has ruled in a 2023 landmark case judgment that a crypto asset is a personal property right that can be claimed or enforced by action and is capable of being subject to a trust.

Cryptocurrency regulation

Cryptocurrencies are either regulated or unregulated under the PSA. However, given that cryptocurrencies have a wide range of attributes, characteristics and features, some cryptocurrencies could fall outside of the ambit of the PSA. Also, some could fall within the purview of Singapore's Securities and Futures Act 2001 ("**SFA**") if their characteristics and features are sufficiently similar to those of capital markets products or securities as defined in the SFA.

Before conducting any cryptocurrency-related activities in Singapore, one should obtain a legal opinion from a Singapore law firm to determine whether and how such activities would be regulated under Singapore law.

The PSA requires a person who carries on a business of providing a payment service to obtain a payment licence. There are seven payment services defined in the PSA, namely: account issuance service; e-money issuance service; cross-border money transfer service; domestic money transfer service; merchant acquisition service; DPT service; and money-changing service.

A cryptocurrency may fall within the definition of "e-money" or "digital payment token", and so a person who carries on a business of providing a payment service in relation to such a cryptocurrency would need to obtain a licence under the PSA. "E-money" is defined as "any electronically stored monetary value that is denominated in any currency, or pegged by its issuer to any currency, has been paid for in advance to enable the making of payment transactions through the use of a payment account, is accepted by a person other than its issuer and represents a claim on its issuer, but does not include any deposit accepted in Singapore, from any person in Singapore". If a person issues e-money for the purpose of allowing another person to make payment transactions, the former would be carrying on an e-money issuance service.

A "digital payment token" is defined as "any digital representation of value (other than an excluded digital representation of value) that is expressed as a unit, is not denominated in any currency, and is not pegged by its issuer to any currency, is, or is intended to be, a medium of exchange accepted by the public, or a section of the public, as payment for goods or services or for the discharge of a debt, can be transferred, stored or traded electronically, and satisfies such other characteristics as MAS may prescribe".

A DPT service may be a service of dealing in DPTs or a service of facilitating the exchange of DPTs.

"Dealing in digital payment tokens" refers to the buying or selling of that DPT in exchange for any money or any other DPT other than facilitating the exchange of DPTs and accepting or using any DPT as a means of payment for the provision of goods or services.

"Facilitating the exchange of digital payment tokens" means "establishing or operating a digital payment token exchange, in a case where the person that establishes or operates that digital payment token exchange, for the purposes of an offer or invitation to buy or sell any

digital payment token in exchange for any money or any digital payment token, comes into possession of any money or any digital payment token, whether at the time that offer or invitation is made or otherwise".

Notwithstanding the above, certain cryptocurrencies that fall within the definition of limited purpose DPT would not be regulated under the PSA. A limited purpose DPT refers to "any non-monetary customer loyalty or reward point, any in-game asset, or any similar digital representation of value that cannot be returned to its issuer, transferred or sold in exchange for money and may only be used in the case of a non-monetary customer loyalty or reward point — for the payment or part payment of, or in exchange for, goods or services, or both, provided by its issuer or any merchant specified by its issuer or in the case of an in-game asset — for the payment of, or in exchange for, virtual objects or virtual services within an online game, or any similar thing within, that is part of, or in relation to, an online game".

In this regard, a non-monetary customer loyalty or reward point refers to "any digital representation of value, by whatever name called, that is not denominated in any currency, is issued as part of a scheme, the dominant purpose of which is to promote the purchase of goods, or the use of services, provided by its issuer or any merchant specified by its issuer, is issued to a person upon the purchase of goods, or the use of services, provided by its issuer or any merchant specified by its issuer, is used for the payment or part payment of, or in exchange for, goods or services (or both) provided by its issuer or any merchant specified by its issuer and is not part of a financial product".

There are two types of licences applicable in relation to cryptocurrencies under the PSA; namely, the standard payment institution licence and the major payment institution licence. A person who is required to obtain a licence for certain payment services (account issuance service, domestic money transfer service, cross-border money transfer service, merchant acquisition service, and/or DPT service) under the PSA would need to obtain a major payment institution licence if the average, over a calendar year, of the total value of all payment transactions that are accepted, processed or executed by the licensee in one month exceeds S$3 million or its equivalent in a foreign currency, for any one of those payment services, or S$6 million or its equivalent in a foreign currency, for two or more of those payment services.

A person who is required to obtain a licence for an e-money issuance service would need to obtain a major payment institution licence if (1) the sum of the average, over a calendar year, of the total value in one day of all e-money that is stored in any payment account issued by the licensee to a person whom the licensee has determined, according to such criteria as MAS may specify by notice in writing, to be resident in Singapore and the average, over a calendar year, of the total value in one day of all e-money that is issued in Singapore, and is stored in any payment account issued by the licensee to any person whom the licensee has not determined, according to such criteria as the Authority may specify by notice in writing, to be resident outside Singapore, exceeds S$5 million, or (2) the average, over a calendar year, of the total value in one day of all specified e-money that is issued by the licensee exceeds S$5 million or its equivalent in a foreign currency.

Other than in the above circumstances, the payment service provider would only need to obtain a standard payment institution licence.

The PSA prescribes the eligibility requirements for applicants to be granted a licence, as well as ongoing compliance requirements for licensees. Eligibility requirements include a minimum base capital of S$100,000 for the standard payment institution licence and S$250,000 for the major payment institution licence. The licence applicant is also required

to have at least one executive director who is a Singapore citizen or Permanent Resident, or else at least one non-executive director who is a Singapore citizen or Permanent Resident and at least one executive director who is a Singapore employment pass holder. Further, the licence applicant must have a permanent place of business or a registered office in Singapore, at which it must keep books of all its transactions in relation to the payment services it provides.

Also, a payment institution needs to appoint at least one person to be present at its permanent place of business or registered office to address any queries or complaints.

While major payment institutions are required to maintain a security amount with MAS for the performance of its obligations to its payment service customers, amendments to the PSA introduced in 2021 would empower MAS to prescribe, where necessary, additional classes of licensees conducting specific payment services to be subject to the requirement to safeguard customer money. Hence, a standard payment institution may be subject to the same requirement.

Under the SFA, cryptocurrencies could potentially have similar features to the conventional types of capital markets products, such as securities, units in collective investment schemes, derivatives contracts, and spot foreign exchange contracts for the purposes of leveraged foreign exchange trading. Securities would include shares, units in a business trust or any instrument conferring or representing a legal or beneficial ownership interest in a corporation, partnership or limited liability partnership, and debentures.

Hence, the conventional requirements could also apply to such cryptocurrencies, depending on the type of activity that is being carried out in relation to such cryptocurrencies. For example, for cryptocurrencies that constitute capital markets products, a person who, whether as principal or agent, carries on or holds himself out as carrying on, a business in "(whether as principal or agent) making or offering to make with any person, or inducing or attempting to induce any person to enter into or to offer to enter into any agreement for or with a view to acquiring, disposing of, entering into, effecting, arranging, subscribing for, or underwriting any capital markets products" would need to hold a capital markets services licence for dealing in capital markets products, while a person who makes an offer of cryptocurrencies that constitute securities or securities-based derivatives contracts would need to prepare and lodge a prospectus with MAS.

For cryptocurrencies that are asset-backed in nature, there is the potential of trading in such cryptocurrencies constituting spot commodity trading under the Commodity Trading Act 1992, and a licence would have to be obtained in order to carry on such an activity.

Cryptocurrencies that exhibit the features of products regulated under Singapore law are not prohibited in Singapore, but the parties that carry on business activities in relation to such cryptocurrencies would have to ensure compliance with the applicable laws. Parties that carry on business activities in relation to cryptocurrencies that do not exhibit the features of the products regulated under Singapore law would be able to do so without restriction, subject to compliance with other general laws of Singapore.

MAS has been continually seeking to ensure that Singapore's regulations keep abreast of the developments in the global cryptocurrency industry and account for the risks and opportunities that come with these developments.

MAS issued a consultation paper on 3 July 2023 to seek public feedback on the draft amendments to the Payment Services Regulations 2019 that would require DPT service providers to safekeep customer assets under a statutory trust and restrict DPT service

providers from facilitating lending and staking of DPT tokens by their retail customers. The former is meant to facilitate the recovery of the customers' monies in the event of the service providers' insolvency. MAS also issued another consultation paper on 3 July 2023 proposing requirements for DPT service providers to address unfair trading practices.

Sales regulation

The sale of cryptocurrencies may be regulated, depending first on whether the cryptocurrencies constitute products regulated under the PSA or SFA. If a cryptocurrency is a security, securities-based derivatives contract or unit in a collective investment scheme, then if a person intends to offer it for sale, it would need to prepare and lodge a prospectus, unless the sale falls within an exemption under the SFA, such as a private placement or a small offer exemption.

A private placement under the SFA requires, among other things, the offers to be made to no more than 50 persons within any period of 12 months. A small offer under the SFA requires, among other things, the total amount raised from the offers within any period of 12 months not to exceed S$5 million or its equivalent in a foreign currency.

If a person intends to act as a broker for the sale or purchase of such a cryptocurrency, then it would need to obtain a capital markets services licence for dealing in capital markets products.

If a cryptocurrency constitutes a DPT under the PSA, then if a party carries on a business of buying or selling it in exchange for money or another DPT, then the party would be providing a DPT service of dealing in DPTs. Hence, this party would need to obtain a licence under the PSA to do so in Singapore.

If a cryptocurrency constitutes e-money under the PSA, then if a party carries on a business of issuing it to any person for the purpose of allowing the person to make payment transactions, then the party would be providing an e-money issuance service under the PSA and would need to obtain a licence under the PSA to do so in Singapore.

Other than addressing the regulatory issues, persons who issue or sell cryptocurrencies in Singapore would need a robust set of legal documentation under Singapore law to govern the transactions and to set out the rights and obligations between the sellers/issuers and the purchasers. This is important for protecting each party's rights and interests. Important legal documentation includes Token Sale Terms and Conditions, a Privacy Policy, an Anti-Money Laundering/Counter-Financing of Terrorism Compliance Manual, a Simple Agreement for Future Tokens, a Private Placement Memorandum, and a Prospectus.

Taxation

Taxation of cryptocurrency in Singapore depends on the type of activity that is being carried out. Where trading in cryptocurrency is carried out in the ordinary course of business, the profit derived therefrom would be subject to income tax. Where cryptocurrencies are purchased for long-term investment purposes, capital gains derived therefrom would not be subject to tax as Singapore does not impose taxes on capital gains.

Where cryptocurrencies are used to pay for goods or services, the business providing the goods or services would be taxed on the value of the said goods or services. This is because cryptocurrencies are not fiat currencies and not legal tender. Furthermore, cryptocurrencies would be treated as intangible property for the purposes of income tax. Hence, transactions with cryptocurrencies being used as payment would be considered barter trade.

The Inland Revenue Authority of Singapore has indicated in its e-Tax Guide on Income Tax Treatment of Digital Tokens that the taxability of proceeds from an initial coin offering ("**ICO**") depends on the type of coin being issued. If the coin is a payment token, then generally it would be treated as trading stock and the ICO proceeds would be taxable. If the coin is a utility token, then because there is an obligation for the issuer to provide a service in the future, the ICO proceeds would represent consideration for the service and would be taxable when the services are performed. If the coin is a security token, then the ICO proceeds would be treated as those arising from the issuance of investment assets, and being capital in nature, it would not be taxable.

Money transmission laws and anti-money laundering requirements

General anti-money laundering laws apply to cryptocurrencies in Singapore. The Corruption, Drug Trafficking and Other Serious Crimes (Confiscation of Benefits) Act 1992 ("**CDSA**") provides for the obligation to report suspicious transactions with the Suspicious Transaction Reporting Office, Commercial Affairs Department of the Singapore Police Force as soon as is reasonably practicable. A failure to file a Suspicious Transaction Report would constitute a criminal offence under the CDSA.

Under the Terrorism (Suppression of Financing) Act 2002 ("**TSFA**"), a person should disclose to the police any possession, custody or control of any property belonging to any terrorist or terrorist entity, or any information about any transaction or proposed transaction in respect of any property belonging to any terrorist or terrorist entity in accordance with the First Schedule of the TSFA. A person should also ensure that it complies with the financial sanction requirements in relation to the designated individuals and entities pursuant to the TSFA, as set out on the website of the Ministry of Home Affairs, and the various regulations giving effect to the United Nations Security Council Resolutions.

If a person is regulated under the SFA, Notice SFA04-N02 "Prevention of Money Laundering and Countering the Financing of Terrorism – Capital Markets Intermediaries" could apply to the person.

If a person is regulated under the PSA, Notice PSN01 "Prevention of Money Laundering and Countering the Financing of Terrorism – Holders of Payment Services Licence (Specified Payment Services)" and/or Notice PSN02 "Prevention of Money Laundering and Countering the Financing of Terrorism – Holders of Payment Services Licence (Digital Payment Token Service)" issued by MAS could apply to the person. With the 2021 PSA amendments, which are to come into operation on a date appointed by the minister, the definition of DPT services would be expanded to include the transfer of DPTs, the provision of custodian wallet services for DPTs, and facilitating the exchange of DPTs without possession of monies or DPTs by the DPT service provider. Such virtual asset service providers and crypto intermediaries may also now come under the regulatory ambit of MAS. The definition of a "cross-border transfer service" has also been further tightened and broadened to include the activity of facilitating transfers of money between persons in different jurisdictions even when money is not accepted or received by the service provider in Singapore; service providers must still be licensed and are subject to rules and regulations set by MAS even if the monies do not flow through Singapore. This is an interesting development because an entity domiciled in Singapore that may have a minimal role in a cross-border transfer transaction may require itself to be regulated in Singapore in order to be part of the cross-border transfer "ecosystem" of a global money transfer service.

Furthermore, under the FSM Act, all entities created or operating in Singapore who conduct a business of providing digital token services completely outside of Singapore will also be regulated for money-laundering and terrorism-financing risks. The scope of digital token services under the FSM Act includes facilitating the exchange of digital tokens, inducing or attempting to induce a person to enter into any agreement for digital tokens in exchange for money or other digital tokens, and providing financial advice relating to the offer or sale of digital tokens. The FSM Act is coming into force in phases, and the part of the FSM Act that enhances the regulation of digital token service providers for money laundering and terrorist financing risks is targeted to be implemented between the second half of 2023 and 2024.

In addition, DPT service providers may be subject to additional requirements that MAS considers necessary or expedient to prescribe in the interest of the public, the stability of the financial system in Singapore, or the monetary policy of MAS. MAS may impose at its discretion a requirement for the DPT service provider to procure a banker's guarantee, professional indemnity insurance or even to lodge a security deposit with MAS prior to MAS issuing the operating licence to the DPT service provider. MAS is also empowered to impose user protection measures on DPT service providers where necessary. A notable example would be a requirement for the DPT service provider to segregate customer assets from its own assets or to restrict a DPT service provider from moving customer assets out of one entity to another regardless of where the entity is situated.

A person who is regulated and licensed under the SFA or PSA ("**Licensee**") should generally identify the customer, as well as the legal form, constitution and powers that regulate and bind the legal person or legal arrangement, and understand the nature of the customer's business and its ownership and control structure. The Licensee should verify the identity of the customer using reliable, independent source data, documents or information. Where the customer is a legal person or legal arrangement, the Licensee should verify the legal form, proof of existence, constitution and powers that regulate and bind the customer, using reliable, independent source data, documents or information.

The aforesaid measures and guidelines are not exhaustive. The Licensee should refer to the entire set of MAS Notices and Guidelines, as applicable, to ensure compliance with anti-money laundering/counter-financing of terrorism measures.

Promotion and testing

MAS has implemented a regulatory sandbox programme in order to provide financial institutions and start-ups with a conducive regulatory environment for technological innovation in the rapidly evolving financial technology space.

The sandbox for each participant would have specified boundaries and duration. There would be safeguards to protect against the implications of failure on the overall financial system. Specific legal and regulatory requirements as determined by MAS will be relaxed for the participant while the sandbox is in effect. After exiting the sandbox, the participant would then have to ensure complete compliance with the full extent of its legal and regulatory requirements.

MAS has indicated in the Fintech Regulatory Sandbox Guidelines updated in January 2022 that some examples of legal and regulatory requirements that it is prepared to consider relaxing for the purpose of the sandbox are asset maintenance, board composition, cash balances, credit rating, financial soundness, fund solvency and capital adequacy, licence fees, management experience, MAS Guidelines for technology risk management and outsourcing, other MAS Guidelines, minimum liquid assets, minimum paid-up capital,

relative size, reputation, and track record. MAS has also indicated that some examples of legal and regulatory requirements that it intends to maintain are the confidentiality of customer information, fit and proper criteria particularly on honesty and integrity, handling of customers' monies and assets by intermediaries, and prevention of money laundering and countering the financing of terrorism.

Various government agencies in Singapore, such as the National Research Foundation, the Agency for Science, Technology and Research, the Defence Science and Technology Agency, Enterprise Singapore, GovTech Singapore, the Infocomm Media Development Authority, and MAS, together with various universities in Singapore, are also collaborating under the Singapore Blockchain Innovation Programme ("**SBIP**"). The purpose of the SBIP is to strengthen Singapore's blockchain ecosystem through engaging local companies in blockchain-related projects and business solutions, growing and nurturing Singapore's blockchain community and talent pool, and conducting research on blockchain scalability and interoperability.

Ownership and licensing requirements

If a cryptocurrency's features cause it to fall within the definition of a capital markets product, then a person who is "making or offering to make with any person, or inducing or attempting to induce any person to enter into or to offer to enter into any agreement for or with a view to acquiring, disposing of, entering into, effecting, arranging, subscribing for, or underwriting" such a cryptocurrency would be carrying on a regulated activity of dealing in capital markets products. Such a person would need to obtain a capital markets services licence under the SFA in order to carry on business in this regulated activity.

Where a cryptocurrency forms part of the property of a collective investment scheme, a person who manages the property or operates this collective investment scheme would be carrying on the regulated activity of fund management. If a person undertakes on behalf of a customer the management of a portfolio that contains any cryptocurrency that constitutes a capital markets product, the person would be carrying on the regulated activity of fund management. In this regard, a person who carries on business in fund management would need to obtain a capital markets services licence under the SFA to do so.

Where a cryptocurrency constitutes an investment product under the Financial Advisers Act 2001, which includes capital markets products, a person who provides a financial advisory service on such a cryptocurrency would need to obtain a financial adviser's licence in order to act as a financial adviser in Singapore in respect of such financial advisory service.

Mining

At present, there are no pieces of regulatory legislation or prohibitions directly applicable to crypto mining as an activity. However, profits arising from operations that mine cryptocurrencies in exchange for money are subject to income tax.

To the extent that the cryptocurrency being mined constitutes a regulated product, then depending on the specific mining arrangement, it may fall under the regulatory ambit of the SFA.

Border restrictions and declaration

There are currently no border restrictions or declarations required with respect to crypto-currencies.

Reporting requirements

For unregulated entities, they would have to comply with the reporting requirements under the CDSA and the TSFA.

For an entity licensed under the PSA, it would need to comply with the MAS Notice on Reporting of Suspicious Activities and Incidents of Fraud (PSN03) by lodging with MAS a report no later than five working days after the discovery of any suspicious activities or incidents of fraud where such activities or incidents are material to the safety, soundness or reputation of the entity.

A licensee under the PSA would also have to comply with the MAS Notice on Prevention of Money Laundering and Countering the Financing of Terrorism – Holders of Payment Services Licence (Specified Payment Services) (PSN01) or the MAS Notice on Prevention of Money Laundering and Countering the Financing of Terrorism – Holders of Payment Services Licence (Digital Payment Token Service) (PSN02), as applicable.

Under the PSN01, a payment service provider would need to perform certain prescribed customer due diligence measures if it undertakes a transaction of a value exceeding S$5,000 for any customer who has not otherwise established business relations with the payment service provider. Payment service providers also may not, in respect of a withdrawal of a payment account in the course of carrying on a business of providing an account issuance service, pay any cash in an amount that is equal to or exceeds S$20,000 to any recipient.

Under the PSN02, a payment service provider may not, in respect of a payment transaction processed, accepted, or executed in the course of carrying on its business to provide a specified payment service, pay any cash in an amount that is equal to or exceeds S$20,000 to any recipient.

Capital markets intermediaries such as holders of a capital markets services licence and registered fund management companies under the SFA would need to comply with the MAS Notice on Prevention of Money Laundering and Countering the Financing of Terrorism – Capital Markets Intermediaries (SFA04-N02).

Under the SFA04-N02, a capital markets intermediary shall perform prescribed customer due diligence measures when it undertakes any transaction of a value exceeding S$20,000 for any customer who has not otherwise established business relations with it.

Estate planning and testamentary succession

The main pieces of legislation in the area of estate planning and testamentary succession, which are the Intestate Succession Act 1967, the Wills Act 1838, and the Probate and Administration Act 1934, have no specific laws dealing with cryptocurrencies.

Hence, generally, an owner of cryptocurrencies should specifically mention the cryptocurrencies in a will, otherwise the executors and beneficiaries may not even know about their existence. Furthermore, the testator should provide for the cryptocurrencies' access information, such as the private key details and wallet passwords to be disclosed to the executors or beneficiaries privately, otherwise there would be little recourse for the executors or beneficiaries to retrieve the cryptocurrencies due to their decentralised nature.

An owner of cryptocurrencies may also create a trust over the cryptocurrencies for his/her beneficiaries, and could then appoint a professional to manage the cryptocurrencies as trust property.

Kenneth Pereire
Tel: +65 6916 1299 / Email: kenneth@kgplegal.com.sg

Mr Kenneth Pereire is a corporate and commercial lawyer and the Managing Director of KGP Legal LLC. He obtained his qualifications as a Singapore lawyer in 2011 and has worked in Singapore and the ASEAN region for the past 10 years. His work covers the full range of general corporate and commercial law matters, from mergers and acquisitions and cross-border transactions for international and multi-national companies, including securities and other regulatory and compliance matters, down to the day-to-day legal concerns of small and medium-sized enterprises in establishing operations, drafting all kinds of commercial contracts, licensing and distribution arrangements, employment law matters, leasing, intellectual property registration and protection and litigation advice and assistance.

Lin YingXin
Tel: +65 6916 1295 / Email: yingxin@kgplegal.com.sg

Mr Lin YingXin is a corporate and commercial lawyer and an Associate Director of KGP Legal LLC. He was admitted to the Singapore Bar in 2015. He has worked on numerous local and cross-border transactions and disputes, and has advised entrepreneurs, investors, shareholders, directors, start-ups, small and medium-sized enterprises, and multi-national corporations from various industries, including financial technology, finance, education, biotechnology, software development, distribution, blockchain and cryptocurrency, and e-commerce. His practice focuses on general corporate and commercial law, including mergers and acquisitions, corporate finance, employment law as well as regulatory and compliance matters. He regularly assists clients in reviewing, negotiating and drafting various types of contracts and documentation.

KGP Legal LLC

10 Anson Road, #23-05, International Plaza, Singapore 079903
Tel: +65 6916 1298 / URL: www.kgplegal.com.sg

Spain

Alfonso López-Ibor Aliño & Olivia López-Ibor Jaume
López-Ibor Abogados, S.L.P.

Government attitude and definition

The Spanish government has been cautious and conservative regarding cryptocurrencies, since Spanish law is highly protective of the rights of investors and consumers, and because, during the recession, there were a number of cases of financial, securities and crypto-asset fraud. Cryptocurrency cannot be legally treated as money for legal tender. Law 46/1998, of December 17, on the introduction of the euro as the national currency, provided that from January 1, 1999, the national currency of Spain shall be the euro. In this sense, in January 2023, Spanish fintech company MONEI was given the green light by the Bank of Spain to carry out its digital euro project, which was showcased in the Spanish financial sandbox. Under the name EURM, this stablecoin will be the first digital euro in Europe. EURM facilitates the transmission of euros between individuals and online payments through the creation of a token using the new Ethereum 2.0 blockchain technology. This shows an intention from the Bank of Spain not to fight blockchain technology but to embrace it and gain a spotlight in it.

In relation to anti-money laundering ("AML") matters, on April 28, 2021, the Spanish National Gazette published Royal Decree 7/2021, of April 27, for the transposition of the EU directives on the areas of competition, prevention of money laundering and credit institutions. This Royal Decree modified Law 10/2010, of April 28, for the Prevention of Money Laundering and Financing of Terrorism, which has been a strong topic of concern for all governments in relation to crypto-assets being used in bad faith. The most relevant inclusions were an official definition for virtual assets and new regulated entities included within article 2 of Law 10/2010, among which we can find, in section z), the "providers of services regarding the exchange between virtual and fiat currency, and the custody of virtual wallets" (hereinafter, "Virtual Currency Service Providers"). This means that all Virtual Currency Service Providers must be registered within the Bank of Spain's Registry specifically tailored for these types of entities.

The Registry has been active since January 2022 and, to date, 80 entities that now operate in Spain have been registered.

Furthermore, Law 6/2023, of March 17, of the Securities Markets and Investment Services entered into force on April 2023 ("new LMV"). This new law establishes that all financial instruments that are issued, registered, transferred, or stored using distributed ledger technology ("DLT") or other similar technologies will be subject to the new LMV. Additionally, it also appoints the National Stock Market Commission ("CNMV") as the competent authority to oversee compliance on the European Commission's regulation on Markets in Crypto-Assets ("MiCA").

Lastly, Law 28/2022, of December 21, on the promotion of the start-up ecosystem ("Start-up Law") entered into force on December 22, 2022, and although it is not tailored specifically to blockchain technology, start-up companies that are innovating with this technology will benefit from it. Besides tax benefits and other facilitators introduced, the Start-up Law also regulates controlled test environments, known as regulatory sandboxes. The purpose of these spaces is to exempt the general regulations under the supervision of a regulatory body or entity and to evaluate the usefulness, viability, and impact of technological innovations in the different sectors of productive activity. In this case, start-ups are allowed to test for one year, in an environment controlled by the corresponding regulator.

Spain is actively working towards attracting entrepreneurs, venture capitalists, and corporate venture capitalists by establishing an efficient legal framework that promotes the seamless integration of blockchain technology. This approach facilitates innovation and presents compelling solutions to current challenges in the worlds of finance and data protection. Several recent developments contribute to this objective, including the publication of MiCA, the introduction of the new LMV, the enactment of the Start-up Law, and the application of AML provisions to Virtual Currency Service Providers.

Cryptocurrency regulation

As discussed above, Spain lacks a specific regulatory framework for DLT/blockchain and cryptocurrencies. However, Spanish law, through Royal Decree 7/2021 (see "Government attitude and definition" above), has regulated providers of crypto-to-fiat currency (and *vice versa*) exchange and custodian services from the standpoint of AML legislation and introduced a definition for virtual currencies.

On another note, while cryptocurrencies are not considered legal tender or financial instruments in Spanish law, they can be treated as securities in the case of public offerings, or as chattels or commodities when traded individually.

To the extent that cryptocurrencies can be considered securities, initial coin offerings may fall within the prospectus-filing requirements of the new LMV, as the definition of financial instruments and negotiable securities is very wide (article 2 of the new LMV). This was confirmed by the CNMV through a *communiqué* published back in 2018 and more recently by the entering into force of the new LMV, which, as stated in "Government attitude and definition" above, drags under its scope all financial instruments that are issued, registered, transferred or stored using DLT or other similar technologies.

To address the need for regulation, MiCA was published in the Official Journal of the European Union on June 9, 2023. During the adaptation period, the CNMV and the Bank of Spain will play a crucial role in implementing indirect regulations related to cryptocurrencies in Spain. Article 247 of the new LMV, for example, empowers the CNMV to establish prerequisites for cryptocurrency advertising and remove fraudulent or misleading advertisements (these prerequisites and conditions were outlined within Circular 1/2022, of January 10, of the CNMV, regarding the advertising of crypto-assets presented as investment objects). The new LMV also designates the CNMV as the competent authority for supervising MiCA compliance.

Sales regulation

To the extent that cryptocurrencies are considered commodities, they will be traded under the general rules of the Civil Code and the Code of Commerce, particularly those applicable to the contract of barter (permute). MiCA, as discussed above, was recently published on

June 9, 2023, marking an important transition point towards the digitalisation of traditional economy. It is important to note that, even though it has already entered into force, MiCA will only be applicable from December 30, 2024 onwards.

MiCA will stir up the whole regulation concerning sales in the crypto sphere. Aside from Spanish law that would allow the parties freedom of choice of the governing law applicable to the transaction (article 3 of Rome I, Regulation (EC) 593/2008 on the law applicable to contractual obligations), small investors qualify for treatment as consumers and therefore, even if a law other than Spain's has been chosen, mandatory Spanish law on consumer or investment protection will apply to the trade in order to benefit the Spanish party (article 6.2 of Rome I), which expressly refers to the "protection afforded by legal provisions that cannot be derogated from by agreement (…)". Depending on the type of tokens (security or utility), the Spanish rules on title transfer may be easier or more difficult to apply. Broadly speaking, Spanish law requires a contractual agreement plus the delivery of the object, so that title is passed from the seller to the purchaser. This would be non-controversial if the security token comprised only membership rights within the meaning of corporate law, but would be different and more complicated in the case of dematerialised claims, such as payment claims made via the internet. Thus, much depends on how Spanish law characterises cryptocurrencies. According to Law 10/2010, virtual currencies are a "digital representation of value not issued by a central bank or public authority, which is not necessarily associated to an established legal tender and does not possess the legal status of currency or money but is accepted as medium of exchange and can be transferred, stored or electronically negotiated".

This view is based on the fact of the purchase of a financial instrument, there being a profit expectation, and also the confidence in other people's efforts to generate economic revenue.

Taxation

In April 2023, the Cabinet of Ministers approved Royal Decree 249/2023, of April 4, amending the General Regulations for the Development of the General Tax Law, regarding administrative review, which has as its most relevant introduction the obligation to declare, as of January 1, 2024, the possession of cryptocurrency – and other virtual assets – and operations that are carried out with their use. The modification introduces three obligations:

a. *Obligation to report balances in virtual currencies*: Persons and entities resident in Spain, and permanent establishments in Spanish territory (belonging to individuals or entities residing abroad), that provide services to safeguard private cryptographic keys on behalf of third parties, to maintain, store and transfer virtual currencies, will be obliged to file an annual informative declaration referring to all the virtual currencies they keep in custody.
b. *Obligation to report transactions with virtual currencies*: Persons and entities residing in Spain, and permanent establishments in Spanish territory (belonging to individuals or entities residing abroad), that provide the services described above and services for exchanging virtual currencies and fiat currency or between different virtual currencies, and intermediate in any way in the execution of these operations, will be required to submit an annual informative declaration regarding the acquisition, transmission, exchange, and transfer of virtual currencies, as well as the receipts and payments made in such currencies, in which they are involved or act as intermediaries.
   It is important to note that the above does not apply to individuals or entities that limit their activity to advising on virtual currencies.
c. *Obligation to report virtual currencies located abroad*: All the abovementioned will also have to annually declare all virtual currencies held abroad, either as the owner or, if applicable, as the beneficiary.

To declare cryptocurrencies, the Tax Office has included a section (1800) dedicated to virtual currencies. In this section, all buying and selling transactions must be included, with a maximum limit of 25 capital gains and losses.

Furthermore, in 2024, Form 721 will be introduced, which will replace Form 720, for entities to report on virtual currencies held abroad. In this case, there will be no obligation to report cryptocurrencies if the combined balances as of December 31 do not exceed EUR 50,000.

On the other hand, Forms 172 and 173 will focus on companies with tax residency in Spain that participate in the cryptocurrency market, either as exchange and/or electronic wallet custody providers.

Money transmission laws and anti-money laundering requirements

As discussed above, on April 28, 2021, the Spanish National Gazette published Royal Decree 7/2021. There are several definitions included in the modified article 1 of Law 10/2010, such as that for virtual currencies: "Virtual Currency means any digital representation of value not issued by a central bank or public authority, which is not necessarily associated to an established legal tender and does not possess the legal status of currency or money but is accepted as medium of exchange and can be transferred, stored or electronically negotiated." Furthermore, as also discussed above, new regulated entities have been included within article 2 of Law 10/2010.

Promotion and testing

In November 2020, the Spanish government approved Law 7/2020 on the digital transformation of the financial system, which provided for the creation of a test space specifically tailored for innovations within the financial sector subject to administrative supervision (financial sandbox). It is an attempt to change Spanish regulatory culture by establishing an information centre on technofinance and offering the industry a space to test new products and share experiences. Pilot projects will be selected and supervisors to carry out the follow-up will be appointed, and if testing is satisfactory, licences will be granted. Spanish law seems to be drawing its inspiration from the UK Financial Authority, which grants licences for sandboxes. The aim of this law is to establish a level playing field for banks, Big Tech, and start-ups.

The steps to enter the sandbox are the following:

1. Application: The entry of projects to the sandbox must be requested at the electronic headquarters of the General Secretariat of the Treasury and International Finance. The application must be accompanied by an Annex of required questions and an explanatory Memorandum of the project detailing the business model and the reasons that justify its entry into the controlled testing space.
2. Evaluation: The competent authorities will evaluate the project and details of its application to determine its suitability to access the sandbox. Those that do not meet the requirements will be automatically discarded by means of a reasoned statement.
3. Tests: An entity that is considered suitable to access the sandbox will begin its business activity after the approval of the testing protocol, once the informed consent of the participants has been obtained and the system of guarantees and indemnities foreseen has been activated. The testing period will be for an initial period of six months, which may be extended.

There are currently several DeFi and blockchain projects in the sandbox as well as many other areas, with the most recent highlight being the approval of the digital euro project showcased by MONEI.

Moreover, as mentioned in "Government attitude and definition" above, the Start-up Law entered into force on December 22, 2022, which regulates regulatory sandboxes for innovations beyond the financial sector.

Ownership and licensing requirements

Virtual Currency Service Providers have to comply with the following provisions without prejudice to what is established in accordance with the authorisation requirements imposed by MiCA:

1. Regardless of their nationality, if services relating to "Virtual Currency Exchange for Fiat Currency" or "Services for the Custody of Electronic Wallets" are offered or provided in Spanish territory, these individuals or entities will have to be registered with the Registry of the Spanish Central Bank ("SCB") created for these purposes.
   In this sense, it is important to note that since the applicable local regulations for Virtual Currency Service Providers are AML laws, reverse solicitation is not a viable option for cryptocurrency service providers since this concept is not included in these laws. This is mainly because reverse solicitation is applicable in the case of financial services companies that fall under the Spanish Stock Market Law and the supervision of the CNMV. Regarding regulations at the European level, this concept is set out explicitly only in MiFID II related to investment services.
2. Likewise, the following must also register with the SCB Registry:
   a. Regardless of their nationality, those individuals or entities that provide the aforementioned services, when the address, administration or management of these activities resides in Spain, regardless of the location of the service recipients.
   b. Entities located in Spain that provide these services, regardless of the location of the service recipients.
3. Registration with the SCB Registry is conditioned to the existence of:
   a. Adequate AML prevention procedures, provided by Law 10/2010. In order to comply with this requirement, the following must be filed to the SCB: (i) an AML Procedure Policy (which must contain due diligence measures, KYC policies, identification of clients, communications to SEPBLAC, internal control measures, etc.); (ii) a Risk Analysis Assessment; and (iii) the appointment of a company representative (holding a management position) before SEPBLAC.
   b. Compliance with the requirements of commercial and professional honourability, according to the terms established in article 30 of Royal Decree 84/2015, of February 13, for the development of Law 10/2014, of June 26, on the regulation, supervision, and solvency of credit institutions. In summary, these requirements consist of displaying personal, business, and professional conduct that does not cast doubt on the ability to perform sound and prudent management of the entity.

   The SCB now has the authority to supervise the compliance of the aforementioned requirements.
4. Applicants will also have to file the following forms:
   a. CRIPTO01: For service providers that exchange fiat money for virtual currency.
   b. CRIPTO03: For virtual wallet custody service providers.
   c. CRIPO05: For the evaluation of the suitability of both the company and its directors (a separate form must be signed by each director).
5. Lastly, the following documents are required: the company's Tax Identification Number ("NIF"); and criminal records (no older than three months) for both the company and its directors.

It is important to highlight that if Virtual Currency Service Providers do not comply with the registration requirements above, such conduct could be considered a very serious infringement of Spanish law, and the entity or individual will be subject to sanctions imposed by the SCB. However, the infringement will be considered "not very serious" if the provided services were occasional or isolated.

In relation to this new Royal Decree, it is interesting to note that for the first time, an official definition of virtual assets is offered by Spanish legislation. Previously, consideration of these assets in Spain was limited to the jurisprudential scope of Supreme Court Decision 326/2019, of June 20, 2019, through which the criminal chamber defined them as "intangible assets of exchange" that, in no way, have the legal consideration of fiat money. Through this new Royal Decree, the legislator solidifies the Supreme Court's insight, strengthening its approach and consolidating a definition for virtual assets as a source of Spanish law.

As of July 2023, more than a year after the Registry's creation, approximately 80 companies have managed to become registered. Even though the Bank of Spain has a period of three months to provide a resolution to applications, such period is suspended every time a requirement of additional information or amendment of documents is sent to the applicant.

Mining

There are currently no specific laws, regulations or judicial decisions regulating mining activities in Spain. Similarly, this topic has not been addressed at the European level.

Please see "Taxation" above regarding the tax provisions applicable to earnings originated from activities involving blockchain technology.

Border restrictions and declaration

As mentioned in "Taxation" above, Royal Decree 249/2023 introduced obligations to declare virtual currencies located abroad. This obligation is applicable to persons and entities resident in Spain, and permanent establishments in Spanish territory (belonging to individuals or entities residing abroad), that provide services to safeguard private cryptographic keys on behalf of third parties, to maintain, store and transfer virtual currencies, and/or provide services for exchanging virtual currencies and fiat currency or between different virtual currencies.

As discussed above, in 2024, Form 721 will replace Form 720 for entities to report on virtual currencies held abroad.

Reporting requirements

Systematic reporting requirements

Article 27 of Law 10/2010, approved by Royal Decree 304/2014, of May 5, states that obliged subjects (among which cryptocurrency service providers are now included) shall report to the Spanish AML authority (i.e. SEPBLAC) on a monthly basis in accordance with the following conditions (when applicable):

a. Transactions entailing the physical movement of coins, paper currency, travellers' cheques, cheques or other bearer documents issued by credit institutions, except those that are credited or debited to a customer's account, for amounts exceeding EUR 30,000 or the equivalent amount in foreign currency.
b. Obliged subjects that perform money remittances in the terms set out in article 2 of Law 16/2009, of November 13, on payment services, shall report to SEPBLAC any

transactions entailing the physical movement of coins, paper currency, travellers' cheques, cheques or other bearer documents for amounts exceeding EUR 1,500 or the equivalent amount in foreign currency.

c. Transactions carried out by or with natural or legal persons, or those acting on their behalf, who are resident in territories or countries designated for that purpose by Order of the Minister of Economy and Competitiveness, as well as transactions involving transfers of funds to or from said territories or countries, irrespective of the residence of the persons involved, provided that the amount of those transactions exceeds EUR 30,000 or the equivalent amount in foreign currency.
d. Transactions involving movements of means of payment subject to mandatory declaration under article 34 of Law 10/2010, which include: (i) incoming or outgoing cross-border movements of means of payment for an amount of EUR 10,000 or more or its equivalent in foreign currency; or (ii) movements within national territory of means of payment for an amount of EUR 100,000 or more or its equivalent in foreign currency.
e. Aggregate information about money remittance activity on payment services, broken down by country of origin or destination and by agent or place of business.
f. Aggregate information on international transfers of credit institutions, broken down by country of origin or destination.
g. Transactions specified by Order of the Minister of Economy and Competitiveness.

Additionally, article 34 of Law 10/2010 establishes that a prior declaration shall be made by natural persons who, acting on their own account or for the account of a third party, perform the following movements of means of payments:

- Incoming or outgoing cross-border movements of means of payment for an amount of EUR 10,000 or more or its equivalent in foreign currency.
- Movements within national territory of means of payment for an amount of EUR 100,000 or more or its equivalent in foreign currency.

For these purposes, movement shall mean any change of location or position taking place outside the address of the bearer of the means of payment.

Notwithstanding the foregoing, natural persons acting on behalf of companies that, duly authorised and registered by the Ministry of Interior, engage in the professional transportation of funds or means of payment shall be exempted from the obligation of prior declaration of movements of means of payment.

Lastly, according to Regulation (EU) 2023/1113 of the European Parliament and of the Council, of May 31, 2023, on information accompanying transfers of funds and certain crypto-assets and amending Directive (EU) 2015/849, which was also published on June 9, 2023, Crypto-Asset Service Providers ("CASPs") must, among other things, implement (i) general traceability measures for the transfer of crypto-assets, and (ii) specific traceability measures for the transfer of crypto-assets to or from non-custodial wallets.

The general traceability measures require that the ordering CASP ensures that transfers of crypto-assets are accompanied by certain information about the sender (name, wallet address, country of the crypto-asset account address, official personal document number, client identification number, date and place of birth, or LEI code) and the beneficiary (name, wallet address, crypto-asset account, or LEI code) ("Required Information").

Additionally, the beneficiary CASP must implement effective procedures to detect whether the Required Information is included in or subsequent to the crypto-asset transfer. Before making the crypto-assets available to the beneficiary, the beneficiary CASP will examine the Required Information to verify that the originator or beneficiary is not subject to specific restrictive measures.

The specific traceability measures for the transfer of crypto-assets to or from non-custodial wallets require the CASP to collect and retain the Required Information from their client, verify the accuracy of such information, make it available to the competent authorities upon their request, and ensure that the transfer of crypto-assets can be individually identified. In the case of a transfer of crypto-assets from a non-custodial wallet, the beneficiary CASP will maintain a record of all transfers of crypto-assets from non-custodial wallets and notify the competent authority of any client who has received an amount equal to or exceeding EUR 1,000.

Estate planning and testamentary succession

Cryptocurrency for the purposes of wills and intestate succession will be treated as any other ordinary assets of the deceased person.

Alfonso López-Ibor Aliño
Tel: +34 915 21 78 18 / Email: alfonso.lopezibor@l-ia.com

Alfonso is the Name Partner and founder of López-Ibor Abogados. Before creating the firm, he was the Managing Partner of the Madrid office of Allen & Overy for 10 years, and the Managing Director of the Madrid office of Ventura Garces & López-Ibor Abogados for 18 years, a firm founded by himself together with the late Ventura Garces, a leading commercial lawyer in Barcelona.

His practice covers virtually all aspects of corporate law, finance and banking, aviation law, litigation and arbitration, and mediation. Therefore, throughout his career, he has been involved in a very wide range of subjects, including complex litigation and arbitration.

Alfonso specialises in fintech and blockchain, crypto-assets, and commercial, financial, and banking law. He has experience in syndicated loans, guarantees, and financing of assets, as well as in relationships with the CNMV and the Bank of Spain. He is also recognised for his experience in litigation, arbitration, and air transport law.

In commercial law, he has advised clients on the acquisition and sale of Spanish and foreign companies, in venture capital/private equity transactions, MBOs, and corporate restructuring.

Alfonso oversees the Banking, Finance, and Aviation Department.

Olivia López-Ibor Jaume
Tel: +34 915 21 78 18 / Email: olivia.lopezibor@l-ia.com

Olivia is a Lawyer in the Banking, Finance, and Aviation Department. She began her professional career in the Financial Law Department at Allen & Overy. She has an LL.M. from the Pritzker School of Law (Northwestern University, Chicago).

Olivia specialises in the air transport financing sector and advises aircraft operators and lessors in sale, lease, financing, and mortgage transactions. She also works with airlines and their airport agents in connection with ground attendance administrative procedures.

Olivia advises foreign companies in various securities market operations, including negotiations of guarantees and financing of acquisition packages and CNMV authorisations. She also advises companies engaged in technology in the e-banking sector, payment services, cryptocurrencies, and on the fintech regulatory sector in general.

López-Ibor Abogados, S.L.P.

Calle López de Hoyos, 35, 3, 28002, Madrid, Spain
Tel: +34 91 521 78 18 / URL: www.lopez-iborabogados.com

Sweden

Anders Bergsten, Carl Johan Zimdahl & Carolina Sandell
Mannheimer Swartling Advokatbyrå AB

Government attitude and definition

There is currently no regulation in Sweden specifically directed at cryptocurrencies or crypto-assets and the Swedish Financial Supervisory Authority (Sw. *Finansinspektionen*) (the "**SFSA**") has provided limited guidance on the treatment of crypto-assets.

Cryptocurrency is, however, an increasingly discussed topic in the Swedish parliament and among Swedish governmental authorities. In response to the European Commission's proposal for a new regulatory framework for crypto-assets (known as Regulation 2023/1114 on Markets in Crypto-Assets ("**MiCA**")), the Swedish government has stated that it welcomes a regulation of crypto-assets that promotes responsible innovation, development and competition.

In December 2020, the Swedish government decided to appoint a special investigator with the task of reviewing the government's role in the payment market and deciding what the role should look like in the future. In the report issued by the special investigator (the "**Report**"), it is stated that crypto-assets entail risks mainly for financial stability and that it is important that crypto-assets are subject to an appropriate regulatory framework proportionate to the specific risks that crypto-assets could pose to the financial system and the monetary system as a whole. It is further stated in the Report that, as far as possible, new rules should be anchored in principles and standards set at global level.

Taking the above into consideration, the Swedish government's attitude towards crypto-assets (including cryptocurrencies) should thus not be regarded as negative, although regulations are welcomed to ensure that the use of crypto-assets on a larger scale does not lead to systemic risks and risks for consumers.

In this context, it should be noted that the SFSA has manifested its standpoint that crypto-assets (including cryptocurrencies) are, generally speaking, not suitable for consumer investments due to their speculative nature. Furthermore, the Swedish Consumer Agency (Sw. *Konsumentverket*) has stated that investment in crypto-assets is an area prone to fraud as well as misleading and aggressive marketing activities. Although the authorities are thus generally cautionary in relation to crypto-assets, the statements should be viewed in light of the lack of regulation in the area and the risks posed by such absence of regulation.

Cryptocurrency is not treated as money or given equal status to fiat currency. The Swedish Central Bank (Sw. *Riksbanken*) expressed its opinion on the matter in 2019, ascertaining that it does not regard cryptocurrency as money, also referring to its speculative nature. Hence, the Swedish Central Bank holds the position that "crypto-asset" is a more accurate designation than "cryptocurrency". Furthermore, no cryptocurrencies are currently backed by the government or the Swedish Central Bank.

The Swedish Central Bank is currently investigating the potential launch of an "e-krona", a digital version of the Swedish krona that would be issued by the Swedish Central Bank. The technical solution of the test environment is based on blockchain technology and in April 2021, the first phase of the test was completed. Conclusions from the initial tests were that the examined technology provides opportunity to create uniquely identifiable "e-kronor", although further testing is necessary to ensure, *inter alia*, that mass payments can be handled in the magnitude and with the requirements that a digital central bank currency demands. This, among other issues, such as the technology's compatibility with bank secrecy, will be examined in the next phase of the investigation. The Swedish Central Bank has issued several reports on the project and has continued its work in 2023, investigating how the Swedish Central Bank could cooperate with other players in the payment market to give the public access to and the possibility to pay with e-krona, how conditional payments can be designed and whether digital central bank money can simplify cross-border payments.

However, it should be noted that, to date, there is no formal decision on whether an e-krona will be issued or not and, if so, how it should be regulated and designed and what technical infrastructure and solution it should be based on. The work going forward, before a decision on a possible release, will be less focused on continued technical tests of the specific pilot solution and more weighted towards investigations regarding the design of an e-krona as well as following the international development of digital central bank money. It should also be noted that whether or not an e-krona will be issued is ultimately a political decision.

Within the framework of the e-krona pilot, the Swedish Central Bank has, together with the Bank of Israel, Norges Bank and the Bank for International Settlements ("**BIS**"), tested how the countries' domestic central bank digital currencies' (such as an e-krona) test networks could be integrated to enable and improve cross-currency payments (Project Icebreaker).

The abovementioned Report by a special investigator has also looked into the need for a central bank digital currency. The Report does not currently see sufficiently strong societal needs for the Swedish Central Bank to issue an e-krona. The Report acknowledges, however, that the development is rapid, and thus economic, political and technological changes may prompt a new assessment. Against this background, it is stated in the Report that the Swedish Central Bank should continue to evaluate the basis for introducing an e-krona in order to enable an introduction within a reasonable timeframe in the event that the Swedish government makes such a decision.

Cryptocurrency regulation

There is currently no regulation specifically directed at cryptocurrencies or crypto-assets. However, as of 1 January 2020, a legal or natural person that conducts business in Sweden from a physical entity in Sweden (i.e. a branch, an agent or a Swedish company), which includes professional operations consisting of the management of, or trading in, virtual currency, must be registered in accordance with the Certain Financial Operations Act (Sw. *lag om valutaväxling och annan finansiell verksamhet*) (the "**CFOA**"). A company registered under the CFOA must comply with, for example, the Swedish Anti-Money Laundering and Financing of Terrorism Act (Sw. *lag om åtgärder mot penningtvätt och finansiering av terrorism*) (the "**AML Act**"). The SFSA and the legislator have provided limited guidance in this regard and whether a cryptocurrency/crypto-asset constitutes a virtual currency must consequently be assessed on a case-by-case basis. It may be noted, however, that "virtual currency" is not a defined term in the CFOA, but it has the same meaning as in Directive 2018/84, i.e. "*a digital representation of value that is not issued or guaranteed by a central*

bank or a public authority, is not necessarily attached to a legally established currency and does not possess a legal status of currency or money, but is accepted by natural or legal persons as a means of exchange and which can be transferred, stored and traded electronically" (article 3.18).

Furthermore, depending on the design of the crypto-asset, it may instead fall within the scope of the Electronic Money Act (Sw. *lag om elektroniska pengar*), or the Financial Instruments Trading Act (Sw. *lag om handel med finansiella instrument*). A determination of whether a crypto-asset meets the definition of a financial instrument and, if so, whether or not the services provided should be treated as a regulated service under the Swedish Securities Market Act (Sw. *lag om värdepappersmarknaden*, implementing MiFID 2) must be made on a case-by-case basis. According to the SFSA, this assessment should take into account, *inter alia*, how the cryptocurrencies are electronically registered, their transferability and whether they entail any rights or obligations on behalf of the holder and issuer, respectively. However, due to the lack of guidance, the classification of cryptocurrencies and other crypto-assets is uncertain.

The SFSA as well as certain EU regulators have issued public reports on consumer investments in cryptocurrencies, crypto-assets and financial instruments related thereto, declaring them unsuitable investments for most if not all consumers.

In November 2020, the European Commission proposed a new regulatory framework for crypto-assets, MiCA. The final act was signed on 31 May 2023, and the regulation was published in the Official Journal on 9 June 2023.

Sales regulation

The sale of Bitcoin or other tokens is not specifically or directly regulated, meaning that it will be subject to general provisions regarding securities and commodities under Swedish law.

Taxation

Cryptocurrency is taxed under Swedish legislation upon disposal or in connection with so-called "mining". However, for income tax purposes, cryptocurrencies are generally not characterised as a currency. In a ruling regarding the classification of Bitcoin (HFD 2018 ref. 72), the Swedish Supreme Administrative Court held that currency generally refers to a payment instrument issued and guaranteed by a central bank or similar institution of a state. Bitcoin lacks a formal publisher. Its value is not based on any claim on the issuer but is determined based on market availability and demand. Bitcoin is also not generally accepted as a means of payment. Against this background, the court concluded that Bitcoin cannot be regarded as a foreign currency within the meaning of the Swedish Income Tax Act (the "**ITA**"). Furthermore, Bitcoin cannot be regarded as an equity-related instrument. A sale or other disposal of a Bitcoin (e.g. if Bitcoin is used as payment for goods and services) should therefore be taxed in accordance with the provisions for capital gains and losses on the disposal of "other assets" under the ITA. The Swedish Tax Agency (the "**STA**") has held in a statement that the same should apply for other equivalent cryptocurrencies.

The capital gain or loss on the disposal of a cryptocurrency held as a capital asset is calculated as the difference between the proceeds, after deducting sales costs, and the tax basis. The tax basis for all cryptocurrencies of the same type is calculated together in accordance with the "average cost method" (Sw. *genomsnittsmetoden*). For individuals who are tax resident in Sweden, capital gains are generally taxed as capital income at a rate of 30 per cent, whereas capital losses can only be deducted up to 70 per cent against other capital income.

For Swedish limited liability companies, all income, including taxable capital gains on the disposal of cryptocurrency, is taxed as business income at a rate of 20.6 per cent and any capital losses related to the disposal of cryptocurrency are generally fully deductible.

If cryptocurrency is held as an asset within a trade of business, e.g. as stock in trade, specific tax rules may apply.

Bitcoin and other cryptocurrencies that are received when carrying out so-called "mining" of cryptocurrencies shall normally be taxed as employment income (hobby) for an individual, but could under certain circumstances be taxed as business income. However, even if a cryptocurrency is earned as part of a business activity, the subsequent value change should generally be taxed as capital income for the individual.

For VAT purposes, the provision of exchange services relating to Bitcoin has, however, been considered to fall within the scope of the VAT exemption for currency transactions based on the Court of Justice of the European Union's ruling C-264/14, *Hedqvist* (HFD 2016 ref. 6). The same treatment should also reasonably apply for other equivalent cryptocurrencies.

Money transmission laws and anti-money laundering requirements

The qualification of crypto-assets as financial instruments or e-money implies the applicability of the AML Act in relation to trading or managing crypto-assets, as well as issuing crypto-assets regarded as e-money. Furthermore, the EU's Fifth Anti-Money Laundering Directive is implemented through, *inter alia*, amendments in the CFOA that could be applicable to managers, traders or issuers of crypto-assets (as mentioned above). Crypto-assets falling outside the scope of the abovementioned regulations are not subject to the AML Act.

Promotion and testing

There are currently no Swedish "sandbox" programmes intended to promote research and investment in cryptocurrency. Upon instruction by the Swedish government, the SFSA has established a fintech-specific innovation centre with the purpose of creating a designated space where fintech companies can engage in dialogue with the SFSA and receive information on the regulations applicable to their business, thus facilitating fintech companies' regulatory compliance. The innovation centre is not, however, a regulatory sandbox allowing companies to test their innovations in the market under the SFSA's supervision.

The government, larger financial institutions and private equity firms asked the SFSA to consider the need for a regulatory sandbox in Sweden. The SFSA decided against creating a regulatory sandbox with the argument that innovations in the financial sector are already strong in Sweden and that a regulatory sandbox could adversely affect competition in the market. For the same reason, the SFSA decided not to consider any regulatory changes.

We expect the adoption of blockchain and other distributed ledger technologies to take off in the coming years following the EU's adoption of Regulation 2022/858 on a pilot regime for market infrastructures based on distributed ledger technology (which aims to allow for the development of crypto-assets that qualify as financial instruments and for the development of distributed ledger technology).

Ownership and licensing requirements

There are currently no specific prohibitions on the use or trading of cryptocurrencies in Sweden. However, several restrictions may apply depending on the business and services provided and, as such, the business and services must always be reviewed in light of, primarily, the general regulatory framework on financial services and consumer protection.

An investment advisor advising on financial instruments (which may include crypto-assets) will generally be required to obtain a licence under the Swedish Securities Market Act. Furthermore, a fund manager is generally required to be licensed under the applicable fund legislation, e.g. the Swedish Alternative Investment Fund Act or the Swedish UCITS Act. That being said, there are currently no crypto-specific licensing requirements generally imposed on someone who holds cryptocurrencies.

Mining

Mining cryptocurrencies is currently permitted (and not specifically regulated under Swedish law).

Border restrictions and declaration

As far as we are aware, there are no border restrictions or such to declare cryptocurrency holdings.

Reporting requirements

To our knowledge, there are no such reporting requirements for cryptocurrencies made in excess of a certain value.

Estate planning and testamentary succession

Cryptocurrencies are not specifically regulated or treated in a special way concerning estate planning and testamentary succession under Swedish legislation.

There is no inheritance tax in Sweden, and thus there is generally no need for any specific estate or testamentary succession planning.

Anders Bergsten
Tel: +46 8 5950 6194 / Email: anders.bergsten@msa.se

Anders Bergsten spends a significant part of his practice on drafting, negotiating and managing commercial agreements, particularly IT, technology and outsourcing contracts, support contracts, cloud service contracts, software development contracts, as well as information sharing and cooperation contracts. Anders also regularly advises clients in relation to data protection law matters. He is well versed in EU data protection and cybersecurity law, e.g. the GDPR, the NIS Directive and the Swedish Protective Security Act. Recent examples of the projects in which Anders has been involved include the creation of a major multinational real-time payment, clearing and settlement system, IT projects within the banking and finance industry (including complete back-end outsourcings and custody arrangements), promissory note digitalisation projects, as well as several group-wide IT outsourcings and global industrial IoT projects. The projects in Anders' practice regularly concern multijurisdictional matters with a number of complex technical and legal interfaces in relation to several stakeholders.

Carl Johan Zimdahl
Tel: +46 8 5950 6417 / Email: carl.johan.zimdahl@msa.se

Carl Johan Zimdahl specialises in financial regulation and has extensive experience in advising regulated businesses. His experience covers a wide range of projects including licence applications, fund structuring, fundraisings, restructurings, outsourcings, fit and proper assessments, distribution issues, contract drafting, sanction-related issues and litigation. Recurring clients include Swedish and foreign investment firms, banks, payment institutions, pension funds and managers of private equity funds, debt funds, infrastructure funds, real estate funds and UCITS funds.

Carolina Sandell
Tel: +46 8 5950 6192 / Email: carolina.sandell@msa.se

Carolina Sandell assists clients with advice on regulatory issues, with a particular focus on payment services, electronic money, consumer credits and corporate loans. Carolina's work includes advice in relation to fintech and in connection with permit applications, supervisory matters with the Swedish Financial Supervisory Authority, structural issues and general advice on issues concerning Swedish and EU regulations. Carolina assists both start-ups and established banks, financial institutions, electronic money issuers and payment service providers as well as other companies and entrepreneurs in the financial sector.

Mannheimer Swartling Advokatbyrå AB

Norrlandsgatan 21, 111 87 Stockholm, Sweden
Tel: +46 8 595 060 00 / URL: www.mannheimerswartling.se

Switzerland

Daniel Haeberli, Stefan Oesterhelt & Alexander Wherlock
Homburger

Government attitude and definition

Introduction

In Switzerland, the government's general attitude towards blockchain technology, and in particular towards the tokenisation of securities, is very positive.

Both the Swiss federal government as well as the Swiss Financial Market Supervisory Authority ("**FINMA**") recognise the potential that blockchain and distributed ledger technology ("**DLT**") offer to the financial services industry as well as various other areas of the economy. Switzerland sees an opportunity to take a global lead in this sector, and officials and authorities are generally open *vis-à-vis* new developments.

In December 2018, the Swiss Federal Council published a comprehensive report covering the legal framework for DLT and blockchain in Switzerland.[1] The report generally concluded that Switzerland's legal framework, in principle, already provided for adequate regulations, covering the questions arising in connection with the development of new technologies, such as DLT. However, a need for selective action and improvements in certain areas of private, financial market and insolvency law was identified. In light of these findings, the Swiss Federal Council published a draft law relating to blockchain and DLT ("**DLT-Draft Law**") on March 22, 2019[2] as well as the dispatch to the DLT-Draft Law ("**Dispatch**") on November 27, 2019.[3] On September 25, 2020, the Swiss Parliament approved the Law on Distributed Ledger Technology ("**DLT-Law**"). The DLT-Law constitutes an "umbrella legislation" that introduces a new concept of so-called "DLT-Securities" under the Swiss Code of Obligations allowing for the tokenisation of rights, claims and financial instruments (see below, "Introduction of DLT-Securities"). In addition, the DLT-Law provides for an introduction of a new licensing category as a DLT-Trading Venue under the Financial Market Infrastructure Act ("**FMIA**") (see below, "DLT-Trading Venue") and certain clarifications relating to the treatment of cryptocurrencies in Swiss insolvency proceedings (see below, "Insolvency"). The amendments to the Swiss Code of Obligations and the Federal Act on Intermediated Securities set out under the DLT-Law, which enable the creation of ledger-based DLT-Securities, entered into force on February 1, 2021. Finally, during its meeting on June 18, 2021, the Swiss Federal Council enacted the remaining provisions of the DLT-Law, which, together with the implementing ordinance, entered into force on August 1, 2021.

Definition

Swiss law does not define the terms cryptocurrency or virtual currency. However, the revised Federal Ordinance on Banks and Savings Institutions ("**FBO**") defines the term crypto-based assets (*kryptobasierte Vermögenswerte*) as assets that, pursuant to the intention

of the originator or issuer, were issued with the primary intention to substantially serve as (i) a payment instrument for the acquisition of commodities or services, or (ii) an instrument for money or value transfers.

The definition of the term "crypto-based asset" pursuant to the FBO is of relevance in connection with the determination of whether the acceptance or storage of crypto-based assets triggers a licensing requirement under the Swiss banking regulation (see below, "Licensing requirements"). For the broader treatment of cryptocurrencies under the Swiss financial market regulation, FINMA's "Guidelines for enquiries regarding the regulatory framework for initial coin offerings" ("**ICOs**") ("**FINMA ICO Guidelines**") of February 2018 should be taken into account.[4] Based on this classification, which is also referenced and used by the Swiss Federal Council in the Dispatch,[5] the following three categories of tokens can be distinguished:

- Payment tokens (which are, according to FINMA, synonymous with "pure cryptocurrencies"; referred to herein as "cryptocurrencies") are tokens that are intended to be used, now or in the future, as a means of payment for acquiring goods or services or as a means of money or value transfer. Pure "cryptocurrencies" do not give rise to any claims towards an issuer or a third party. Consequently, according to the prevailing view, such tokens are "purely factual intangible assets".[6] Examples of cryptocurrencies are Bitcoin (including numerous cryptocurrencies resulting from forks or variations of Bitcoin, such as Bitcoin Cash, Bitcoin Gold and Litecoin) and Ether.
- Utility tokens are tokens that are intended to provide access digitally to an application or service by means of a DLT-based infrastructure.
- Asset tokens represent assets such as a debt or an equity claim against the issuer. Asset tokens promise, for example, a share in future company earnings or future capital flows. In terms of their economic function, therefore, such tokens are analogous to equities, bonds or derivatives. Tokens, which enable physical assets to be traded on a blockchain infrastructure, according to FINMA, also fall into this category.

FINMA notes that tokens may also fall into more than one of these three basic categories. Such *hybrid tokens* are, for example, asset tokens or utility tokens, which at the same time also qualify as payment tokens.

Moreover, FINMA published a supplement to the FINMA ICO Guidelines ("**FINMA Supplement**") on September 11, 2019[7] as an answer to an increase of regulatory enquiries in relation to crypto projects using so-called "stablecoins". Generally, a stablecoin is a token whose value is derived from an underlying asset that is considered stable, in order to limit the volatility of the token's price.[8] Such a token can, for example, be linked to an individual or a basket of currencies, real estate, securities or commodities. Examples of such stablecoins are Tether, TrueUSD or DigixDAO. However, other types of stablecoins use stabilisation mechanisms without a direct linkage to any underlying or collateral, as the case may be. Although numerous variations exist, such coins use algorithms or other (automated) systems to stabilise the price of the token by directly or indirectly influencing the demand and supply of the respective token. For example, depending on the current price of the respective token, more tokens may be issued or redeemed on the market.

Cryptocurrencies are not legal tender

In Switzerland, cryptocurrencies do not qualify as legal tender.[9] Consequently, cryptocurrencies are not considered "money" in a narrow sense. However, some legal scholars argue that cryptocurrencies, provided they are widely used, are accepted by the public and have adopted the typical functions of money, qualify as "money" in a broader sense.[10] The Swiss National Bank ("**SNB**"), Switzerland's central bank, does, however, recognise the

potential uses of digital tokens and will continue to closely follow the respective market and technical developments.[11]

There is currently no form of "state-backed" cryptocurrency available in Switzerland. In particular, the SNB has not issued any cryptocurrencies. However, on October 8, 2019, the SNB entered into an operational agreement with the Bank for International Settlements ("**BIS**") regarding the BIS Innovation Hub Centre located in Switzerland. The aim of this Innovation Hub is to gain in-depth knowledge of the relevant technological developments affecting the tasks of central banks. In one of the research projects under this initiative, the integration of digital central bank money into a DLT infrastructure was tested. This new form of digital central bank money may allow the settlement of "tokenised" assets between financial institutions. The project was implemented in the form of a feasibility study as part of a cooperation between the SNB and the SIX Group (Project Helvetia)[12] and successfully demonstrated the feasibility of settling tokenised assets with wholesale central bank digital currencies ("**wholesale CBDC**").[13] In a second phase of Project Helvetia conducted during the fourth quarter of 2021, SNB and SIX Group, together with Citi, Credit Suisse, Goldman Sachs, Hypothekarbank Lenzburg and UBS, assessed and further analysed settlement of interbank, monetary policy and cross-border transactions on the test systems of SIX Digital Exchange ("**SDX**"), the Swiss real-time gross settlement system – SIX Interbank Clearing ("**SIC**") – and core banking systems. On June 10, 2021, the SNB, together with the Banque de France and the BIS Innovation Hub (Project Jura), also announced an experiment regarding the use of digital central bank money for financial intermediaries (wholesale CBDC) to settle cross-border transactions.[14] The project enhances the existing efforts of the G20 regarding cross-border payments. It specifically adds to the development of peer-to-peer adoption, multilateral platforms, and CBDC by providing broader access to the security and stability of central bank money for cross-border settlements. The proposed solution not only addresses current shortcomings but also has the potential to introduce innovative methods for conducting international financial transactions, encompassing foreign exchange ("**FX**"), securities, and other financial instruments.

One of the latest developments is Project Mariana, launched on November 2, 2022, bringing together the Switzerland, Singapore and Eurosystem Centres, with the Bank of France, the Monetary Authority of Singapore and the Swiss National Bank. The project builds on earlier experiments conducted by the BIS Innovation Hub on wholesale CBDCs, incorporating ideas from decentralised finance ("**DeFi**") applications. Its primary aim is to explore the potential of automated market-makers utilising wholesale CBDCs to enhance the efficiency, security, and transparency of FX trading and settlement, thereby reducing certain risks associated with FX markets. Additionally, the project investigated cross-border interoperability using wholesale CBDCs based on a standardised technical framework, ensuring that CBDC developments are adaptable for the future. In the interim report of June 28, 2023, a solution design was presented that could be a promising application in the future.[15]

Moreover, tax authorities in the Canton of Zug started accepting Bitcoin and Ether for tax payments as of 2021, making it the first Swiss canton in which taxes can be paid with cryptocurrencies.[16]

Introduction of DLT-Securities

The DLT-Law introduced a new type of negotiable securities, so-called "DLT-Securities", allowing for the tokenisation of rights, claims and financial instruments, such as bonds, shares, structured products or derivatives. The concept of DLT-Securities aims to ensure the tokenisation of rights by providing the legal framework for an electronic registration of rights that entails the same protection as a traditional security.

The intended purpose of these new ledger-based securities is primarily to allow the issuance and transfer of rights directly on a DLT-based register.[17] Contractual claims (namely under a bond, structured products or other debt instruments) and certain membership rights (*e.g.*, shares in a corporation) both qualify as an admissible underlying of a DLT-Security.[18] Therefore, in particular, asset tokens, such as certain types of stablecoins and certain types of utility tokens, could be issued as DLT-Securities under the DLT-Law.[19] On the other hand, cryptocurrencies (such as, for example, Bitcoin or certain types of stablecoins) that do not give rise to a claim against an issuer and therefore do not have an admissible underlying within the meaning of the DLT-Law, cannot be issued in the form of DLT-Securities.[20]

In order to validly create DLT-Securities, the involved parties (*e.g.*, the issuer of a financial instrument as debtor and the holders of the financial instrument as creditors) must enter into a registration agreement pursuant to which the relevant rights (i) are entered into a so-called "Register of Uncertificated Securities", and (ii) may exclusively be asserted based on and transferred via the register. The register must satisfy certain statutory technical minimum requirements. The register must, namely, exclusively grant the creditors, but not the debtor, actual power of disposal over the respective rights. In addition, the register's integrity must be ensured by implementing adequate technical and organisational protective measures. Pursuant to the DLT-Law, the issuer of DLT-Securities is liable for ensuring that the register functions correctly and that the technical and organisational protective measures are adequately implemented and maintained. The DLT-Law does not specifically define the criteria that the register and respective measures must satisfy. In view of the potential liability of the issuer, it will therefore be of great importance that adequate market standards are developed, *i.e.*, regarding the security and integrity of the register, which can be verified under an audit performed by a third-party service provider.

Cryptocurrency legislation

In Switzerland, cryptocurrency-related activities are not prohibited. Further, subject to the enactment of the DLT-Draft Law, there is currently (apart from the provision in the Swiss Anti-Money Laundering Ordinance mentioned under "Money transmission laws and anti-money laundering requirements", below) no comprehensive tailor-made regulation for cryptocurrencies in effect in Switzerland.

Sales regulation

While offering and selling cryptocurrencies is not subject to specific Swiss sales regulations, an offer and sale of utility tokens, asset tokens and stablecoins may become subject to offer/sales regulations if the tokens in question constitute securities within the meaning of Swiss law.

Under Swiss law, securities (*Effekten*) are financial instruments that are: (i) standardised; (ii) suitable for mass trading; and (iii) either certificated securities (*Wertpapiere*), uncertificated securities (*Wertrechte*), derivatives or intermediated securities (*Bucheffekten*).[21] Whether, or which, tokens qualify as securities is currently not entirely clear, *i.e.*, there is neither any statutory guidance nor any case law regarding this question. Therefore, each token will have to be subject to a specific determination on a case-by-case basis in consideration of the principles outlined by FINMA.

However, in its ICO Guidelines (see above, "Definition"), FINMA indicated that, generally speaking, it does not intend to qualify cryptocurrencies as securities. According to FINMA, utility tokens are not treated as securities if their sole purpose is to confer digital access rights to an application or service, and if the utility tokens can already be used in this manner upon issuance. This view on payment and utility tokens is supported by the Dispatch.[22]

Currently,[23] FINMA has the following view on whether tokens qualify as securities:[24]

- Cryptocurrencies to date are not treated as securities by FINMA. In our opinion, this assessment is correct. Cryptocurrencies do not grant the respective holders or users any relative or absolute rights *vis-à-vis* an issuer or a third party. They serve as mediums of exchange and (arguably) also as units of account and storage of value. Whether cryptocurrencies are "financial instruments" as defined in the recently adopted Swiss Financial Services Act ("**FinSA**").[25] Given the wording of FinSA, we are of the opinion that cryptocurrencies do not qualify as "financial instruments" within the meaning of the cited Act (see below, "Securities firm licence").
- Utility tokens are currently not treated as securities by FINMA, provided that: (i) their sole purpose is to confer digital access rights to an application or service; and (ii) the tokens can actually already be used in this manner when they are issued. If these two conditions are satisfied, the typical "connection with capital markets" inherent to securities, according to FINMA, does not exist. FINMA has clarified that it will qualify utility tokens as securities if they fully or partially "have the economic function of an investment".
- Asset tokens shall, according to FINMA, generally be treated as securities; for example, if they represent uncertified securities or derivatives and are standardised as well as suitable for mass trading. As FINMA points out, uncertificated securities may also be created in so-called pre-financing and pre-sale scenarios, if claims to purchase tokens in the future are granted in the course of such processes. Such uncertified securities will also be treated as securities provided they are standardised and suitable for mass trading.
- Stablecoins, according to the FINMA Supplement, may qualify as securities; for example, stablecoins linked to commodities (other than to so-called precious metals of banks), which give rise to a contractual claim of the holder in relation to such commodities.[26] Also, in the case of a link of a stablecoin to a single security by means of a token holder's contractual delivery claim for such security, a qualification as a security may be possible according to FINMA.[27] Generally, if and to the extent that stablecoins are (i) structured as tokens, whose values are derived from one or more underlying asset(s), and (ii) provide each holder with a contractual claim to the underlying(s), irrespective of whether a physical or cash settlement is provided for (*i.e.*, redemption claim), such tokens may qualify as derivatives within the meaning of FinSA and FMIA (defined above). Since, under Swiss law, stablecoins may qualify as derivatives, such stablecoins may be treated as securities, in particular in the form of uncertificated securities, provided that they are: (i) standardised; and (ii) suitable for mass trading.[28] Moreover, it cannot be excluded that certain types of stablecoins may be qualified as asset tokens by FINMA since, according to FINMA, tokens that enable physical assets to be traded on a blockchain infrastructure also fall into this category (see above, "Introduction"). This might, for example, be the case for stablecoins, which merely fulfil the function of evidencing legal ownership with regard to the respective underlying such as a commodity. However, it must be noted that, from an economical perspective, where asset tokens are linked to underlyings, the respective coin will regularly constitute an indirect investment in such underlying. Conversely, stablecoins use such linkage primarily for the purpose of stabilisation of their price. Therefore, the stabilisation through the link to an underlying is paramount for the qualification as a stablecoin, rather than the (indirect) investment purpose. This is also why relatively stable underlyings such as the U.S. dollar or gold are often chosen. Finally, provided that, from an economical perspective, certain types of stablecoins are designed in a way that they both reflect a payment as well as an investment function purpose, FINMA may qualify such coins as *hybrid tokens*.

On September 29, 2021, FINMA approved a Swiss fund that invests primarily in crypto-based assets for the first time.[29] The fund, the "Crypto Market Index Fund", qualifies as an investment fund according to Swiss law belonging to the category "other funds for alternative investments" with particular risks.

The Crypto Market Index Fund enables qualified investors to participate in this digital asset class. The Crypto Market Index Fund established by "Crypto Finance" tracks the performance of the Crypto Market Index 10, which is administered by the SIX Swiss Exchange. The objective of the Crypto Market Index 10 is to reliably measure the performance of the largest, liquid crypto-assets and tokens and to provide an investable benchmark for this asset class.[30]

Securities firm licence

Sales activities relating to tokens that qualify as securities may in particular trigger: (i) Swiss securities firm licence requirements under the Financial Institutions Act ("**FinIA**");[31] (ii) Swiss trading platform regulations under the FMIA;[32] and/or (iii) Swiss prospectus requirements and further regulations in connection with financial services under FinSA.

- Persons creating certain types of tokens qualifying as securities and/or trading in tokens qualifying as securities on behalf of his/her clients in a professional capacity may qualify as a securities firm under Swiss law and will therefore require a securities firm licence. Moreover, such trading activities relating to tokens qualifying as financial instruments may trigger various regulations under FinSA provided that, among other things, the securities firm is qualified as a "financial service provider". For example, issuing asset tokens in the form of securities, which are linked to the performance of a share or a project, may, under certain circumstances, qualify as regulated securities firm activity. Such issuing activities may also trigger the prospectus requirements under FinSA. The aforementioned licensing requirements under FinIA, however, do not apply as long as the person engaging in such activities has no physical presence (*i.e.*, no personnel and no branch) in Switzerland. Acting on a mere cross-border basis does not trigger any duty to obtain a securities firm licence. However, the regulations under FinSA, in particular, apply to persons who, in a professional capacity, provide financial services in Switzerland or to clients in Switzerland.
- Operating a platform in Switzerland that enables the trading of tokens may trigger licensing requirements under the FMIA. For example, so-called "organised trading facilities" may only be operated by licensed banks, licensed securities firms or recognised (foreign) trading venues. Organised trading facilities are establishments for: (i) multilateral trading in securities or other financial instruments whose purpose is the exchange of bids and the conclusion of contracts based on discretionary rules; (ii) multilateral trading in financial instruments other than securities whose purpose is the exchange of bids and the conclusion of contracts based on non-discretionary rules; and (iii) bilateral trading in securities or other financial instruments whose purpose is the exchange of bids. Even if the types of tokens traded are limited to such that do not qualify as securities under Swiss law, a platform may still be regulated as an "organised trading facility" if the tokens traded are qualified as "other financial instruments". Unlike for "securities", FINMA to date has not yet offered any public guidance on whether they consider cryptocurrencies to be such "other financial instruments".
  As mentioned, FinSA provides for a definition of the term "financial instrument" (see above, "Sales regulation"), which is commonly held to also be relevant for "organised trading facilities". This definition of "financial instrument" is wider than the definition of securities. However, in our view, the wording of the legal definition suggests that cryptocurrencies do not qualify as financial instruments within the meaning of FinSA.

This view seems to be shared by the Swiss Federal Council.[33] Should this view be followed, a platform allowing for the trading of cryptocurrencies such as Bitcoin or Ether would not be considered an "organised trading facility" and would therefore fall outside the scope of the Swiss financial regulations.

DLT-Trading Venue

The DLT-Law also introduced a new licensing category as a DLT-Trading Venue under the FMIA. Licensed DLT-Trading Venues are authorised to provide services in the areas of trading, clearing, settlement and custody of DLT-Securities to both regulated and unregulated financial market participants, including retail investors. Pursuant to the revised Financial Market Infrastructure Ordinance, complex financial products qualifying as DLT-Securities, such as derivatives, may also be admitted to trading on a DLT-Trading Venue, as long as such products do not provide for a time value or a leverage component. Under certain conditions, the trading of cryptocurrencies may also be permitted on a DLT-Trading Venue. DLT-Trading Venues are essentially modelled on the existing traditional trading facilities and are subject to similar requirements (such as stock exchanges and multilateral trading facilities). However, the FMIA provides specific rules for DLT-Trading Venues governing, namely, the admission of participants and the respective DLT-Securities. FINMA is yet to approve a DLT-Trading Venue.

SIX Digital Exchange

In 2021, FINMA issued two approvals to financial market infrastructures that operate based on DLT. SIX Digital Exchange AG has been licensed by FINMA to act as a central securities depository and the associated company SDX Trading AG (collectively, "**SDX**") to act as a stock exchange within the meaning of FMIA.

SDX will offer its participants a fully regulated, integrated trading, settlement, and custody infrastructure based on DLT. This is the first time that a licence has been granted by FINMA to financial market infrastructures that offer trading of digital securities in the form of tokens and provide the integrated settlement services.

Taxation

Cryptocurrencies held by individuals

Wealth tax

For the purpose of tax assessment, cryptocurrencies must be converted into Swiss francs.[34] The Federal Tax Administration ("**FTA**") provides year-end conversion rates for certain cryptocurrencies such as Bitcoin, Ethereum, Ripple, Bitcoin Cash and Litecoin. According to the understanding of different cantonal tax authorities, cryptocurrencies are considered to be assets, comparable with bank deposits, and are therefore subject to wealth taxes. If the FTA does not determine a year-end market value, the cryptocurrencies must be declared at the year-end price of the trading platform via which the buying and selling transactions are executed. If no current valuation rate can be determined, the cryptocurrencies must be declared at the original purchase price in Swiss francs (cost of acquisition). Because the rules for declaring cryptocurrencies can vary, the rules must first be checked in the canton of residence.

Income tax

In general, capital gains on assets of individuals such as cryptocurrencies are exempt from income tax. However, if cryptocurrencies are held as part of the business assets of an individual (*e.g.*, because the individual is classified as a professional securities firm based on the principles laid out in circular no. 36 of the FTA), capital gains of cryptocurrencies are subject to income tax.

In contrast, dividends and interests in periodic form or in the form of one-time compensation on bonds (issue discount and/or redemption premium as the difference between the issue and redemption value) are subject to income tax at the time of realisation.

Cryptocurrencies held by legal entities

Capital tax

Legal entities are subject to annual capital tax. Therefore, legal entities have to declare cryptocurrencies in their tax assessment at cost of acquisition or, if this value is lower, converted at the year-end exchange rate provided by the FTA. Therefore, cryptocurrencies with no market value provided by the FTA are to be declared at acquisition costs.

Corporate income tax

Corporations are subject to Swiss corporate income tax on any net taxable earnings from the sale of cryptocurrencies. Non-realised gains on cryptocurrencies are only subject to Swiss corporate income tax in case of mark-to-market accounting in the Swiss generally accepted accounting principles accounts of the corporate investor.

Value-added tax

For the purpose of value-added tax ("**VAT**"), cryptocurrencies are treated the same way as legal tender, meaning that the trading or exchange activities of cryptocurrencies and additional services related to such trading or exchange activities are exempt from VAT.[35]

Money transmission laws and anti-money laundering requirements

Under Swiss law, both issuing cryptocurrencies as well as the subsequent trading of such tokens may be subject to anti-money laundering regulations.

The relevant starting point is to ask whether a person/company engages in any activities that constitute so-called "financial intermediation" and is hence considered a financial intermediary under the Swiss Anti-Money Laundering Act ("**AMLA**").[36]

There are two main groups of financial intermediaries. First, regulated financial intermediaries belonging to the "banking sector", and second, other financial intermediaries belonging to the "non-banking sector":

- Financial intermediaries belonging to the "banking sector" are companies that are subject to comprehensive, prudential regulation under special legislation, covering the whole range of their activities. Such financial intermediaries are, for example, banks or securities firms.
- Financial intermediaries belonging to the "non-banking sector" are any persons/companies that, on a professional basis: (i) accept or hold deposit assets belonging to third parties; (ii) assist in the investment of such assets; or (iii) assist in the transfer of such assets. This general definition covers, for example, persons/companies that provide services related to payment transactions, hold securities as deposits or manage securities. Whether such activity is carried out in a professional capacity or not must be assessed based on quantitative benchmarks (*e.g.*, gross margin of CHF 50,000 *p.a.*, business relationships with more than 20 parties *p.a.*, unlimited control over third-party assets exceeding CHF 5m at any time, or transaction volume exceeding CHF 2m per calendar year). Prior to engaging in financial intermediation, such persons/companies must join a Swiss self-regulatory organisation.

The AMLA and implementing regulations provide for a series of obligations that financial intermediaries must adhere to, *e.g.*, regarding the verification of the identity of customers/contracting parties as well as the beneficial owners of funds held.

With regard to cryptocurrencies, the following is important concerning anti-money laundering regulations:

- *Primary market/ICOs*: According to FINMA, issuing cryptocurrencies (*e.g.*, payment tokens and/or stablecoins) constitutes financial intermediation (issuance of a means of payment).[37]
- *Secondary market/sales and trading*: Merely selling cryptocurrencies to another party, or using such cryptocurrencies as means of payment for the sale or purchase of goods and services, does not constitute financial intermediation. The revised Swiss Anti-Money Laundering Ordinance, which entered into force in connection with the DLT-Law, clarifies that the assistance provided in connection with the transfer of virtual currencies are services related to payment transactions subject to the AMLA if such services are provided in the context of a permanent business relationship (*dauernde Geschäftsbeziehung*).

Promotion and testing

Switzerland has not established any "sandbox" exemptions or similar arrangements that specifically focus on DLT or cryptocurrencies.

However, there are specific rules in place, which aim at generally promoting FinTech developments in Switzerland.

In 2016, the Swiss government announced that it plans on reducing barriers to market entry for FinTech businesses.[38] This legislative initiative has been implemented and consists of three pillars:

- The first pillar, the Swiss "sandbox" exemption, allows companies to engage in activities that would usually trigger bank licensing requirements. According to the Swiss Banking Act,[39] only licensed banks are permitted to accept deposits from the public in a professional capacity. Any person or entity continuously accepting more than 20 deposits from the public or publicly advertising to accept deposits is deemed to be acting in a professional capacity.[40] Under the sandbox exemption, companies accepting deposits are not considered to be acting in a professional capacity if: (i) the deposits accepted do not exceed the threshold of CHF 1m; (ii) the deposits accepted are neither invested nor interest-bearing; and (iii) the investors are informed in advance, in writing or in another form that provides for a record in text form, that the company is not supervised by FINMA and that the deposits are not protected by the Swiss deposit insurance regime. If the threshold of CHF 1m is exceeded, the company must notify FINMA within 10 days and file for a banking licence.
- The second pillar provides that funds held in customer accounts of asset managers, securities firms, dealers of precious metals or similar companies, which exclusively serve the purpose of settling customer transactions, do not qualify as deposits and therefore do not trigger bank licensing requirements, provided the funds are not interest-bearing and provided that they are forwarded within 60 days. However, FINMA clarified that this "settlement accounts exemption" will not apply to cryptocurrency traders that execute a similar activity as FX traders by maintaining accounts for their clients for investments in different currencies. Under which circumstances a particular activity is considered to be similar to the activities of FX traders is currently not clear.
- The third pillar provides for a so-called "simplified" FinTech licence, which allows the respective licence holder to accept deposits up to the threshold of CHF 100m, provided that the deposits are neither invested nor interest-bearing. The FinTech licence, however,

does not allow the offering and provisions of loans and mortgages. Therefore, it will be predominately crowdfunding platforms that will benefit from the simplified licence. The implementing Ordinance provides for a number of simplified requirements, relating to the required minimum capital, organisation and risk management, which must be satisfied in order to obtain a FinTech licence.

Ownership and licensing requirements

Ownership

Whether tokens can actually be "owned" within the meaning of Swiss ownership laws depends, in particular, on the question of whether they qualify as securities or not. Under Swiss law, it is undisputed that securities can be legally owned. With regard to tokens that do not qualify as securities, *i.e.*, cryptocurrencies such as Bitcoin, the ownership question remains unresolved. The majority of Swiss scholars are currently of the view that, due to their lack of tangibility and for other reasons, cryptocurrencies are not a "thing" (*Sache*) in the sense of Swiss civil law.[41]

Licensing requirements

There are no licences/authorisations specifically relating to cryptocurrencies (*e.g.*, stablecoins) in Switzerland and, therefore, a variety of regulatory licences may be relevant in the area of cryptocurrencies, in particular (but not limited to) the banking licence and the securities firm licence (see above, "Sales regulation").

Under Swiss law, only licensed banks are permitted to accept deposits from the public on a professional basis (see above, "Promotion and testing"). Regulated deposit-taking may become an issue for service providers offering to store customers' cryptocurrencies, in particular. The DLT-Law has clarified under which circumstances the storage of cryptocurrencies requires a licence under the Federal Act on Banks. Thereunder, any person mainly active in the financial markets who, in a professional manner, accepts and stores crypto-based assets within the meaning of the FBO (see above, "Definition") or publicly recommends itself for such services, is required to obtain a FinTech licence (see above, "Promotion and testing"), whereby such crypto-based assets may not be invested nor interest-bearing.[42] Certain exemptions from the licensing requirements apply under the FBO, namely to assets of institutional investors with professional treasury operations. Moreover, for crypto-based assets that banks hold as deposit assets for custodian clients, FINMA may, under the DLT-Law, set a maximum amount on a case-by-case basis if this appears necessary due to the risks associated with such business.[43]

Specifically, with regard to stablecoins, no general statement is possible whether financial market activities in connection with such coins require any financial market licence. The supervisory classification of stablecoins by FINMA follows the following three principles: "substance over form"; "same risks, same rules"; and "case-by-case analysis taking into account the specific circumstances of the individual case".[44] No specific regulations for stablecoins exist in Switzerland. Depending on their design features, stablecoins must therefore be analysed on a case-by-case basis to determine whether any such licence is required. Design features such as (i) whether a single underlying or a basket of underlyings is used, (ii) the type of underlying, as well as (iii) if the stablecoin in question gives the holder a contractual redemption claim with regard to the underlying(s), respectively, the value of the underlying(s), or if the token merely fulfils the function of evidencing an ownership position with regard to the underlying(s), may be decisive.[45] In particular, a banking licence may be required. For example, according to the FINMA Supplement, in particular issuers of

stablecoins that are linked to (i) fiat currency applying a fixed ratio (*e.g.*, 1 token = 1 USD), or (ii) so-called precious metal of banks that provide for a contractual claim for the respective underlying, may require a banking licence.[46] Moreover, among others, for a securities firm, a payment system licence or a licence in connection with collective investment schemes could be required. For instance, FINMA may qualify a currency, security or commodity-linked stablecoin that provides each holder with a redemption claim, whose value is derived from the value of a basket containing various currencies, securities, and commodities, as a collective investment scheme, provided that the underlying assets contained in such basket are managed by the issuer for the account and risk of the token holders. The latter, according to FINMA, mainly means that all opportunities and risks of asset management in the form of profits or losses due to, among other things, interest rates, fluctuations in the value of the underlying assets, and counterparty and operational risks, are borne by the holders of the stablecoin in question.[47] Likewise, stablecoins that are linked to individual properties or a portfolio of properties may, according to FINMA, represent collective investment schemes.[48]

With regard to licensing requirements, it must further be kept in mind that Switzerland implemented the new FinIA along with FinSA in 2020. These new acts set forth a new licensing requirement for individual asset managers and a registration requirement for client advisors. Such registration will be subject to certain requirements such as proof of sufficient education, training and professional experience in the respective area of practice.

Insolvency

Under the former Swiss insolvency regime, it was not sufficiently clear whether crypto-currencies could be segregated in favour of the entitled creditors if a third-party custodian, such as a wallet provider, were to enter into bankruptcy proceedings. In view of these uncertainties, the DLT-Law introduced a new segregation regime that allows the segregation of crypto-assets for the benefit of the relevant creditors and investors in the bankruptcy of the custodian, if certain requirements are met, including, in particular, the following:

- First, the relevant custodian must have an obligation *vis-à-vis* the relevant creditor or investor to keep the crypto-assets available for him at all times. This means that the custodian may, for example, not use such crypto-assets for proprietary business or own-account transactions.
- Second, the crypto-assets will only be segregated if they can be either (i) unambiguously allocated to the individual creditor or investor (however, there will be no need for such allocation to occur directly on the relevant DLT-system itself), or (ii) allocated to a group of investors or creditors and it is evident what share of the joint holdings belongs to a given creditor or investor. The latter option will allow a pooling of crypto-assets held for several creditors or investors.

Therefore, the custody set-up under which the cryptocurrencies are stored is decisive for the question of whether the cryptocurrencies will be segregated in insolvency.

Mining

Switzerland has no laws or regulations that are tailor-made to the phenomenon of cryptocurrencies or mining of cryptocurrencies. Hence, mining of cryptocurrencies is permitted and the activity is not subject to particular laws and regulations.

Since the mere use of cryptocurrencies is not considered financial intermediation (see above, "Money transmission laws and anti-money laundering requirements"), mining of cryptocurrencies does not constitute financial intermediation, as far as it is for personal use.[49] Further, mining of cryptocurrencies does not generally qualify as a financial service within the meaning of FinSA.[50]

Border restrictions and declaration

In Switzerland, there are no particular border restrictions or declaration requirements that would apply to cryptocurrencies.

Reporting requirements

In Switzerland, making payments with cryptocurrencies is not a regulated activity and there are no reporting requirements to be met when such payments are made.

Estate planning and testamentary succession

In Switzerland, there are no particular estate planning or testamentary succession aspects concerning cryptocurrencies.

Under Swiss law, heirs acquire the inheritance as a whole upon death of the testator by operation of law. Therefore, all possessions with an inheritable value are transferred to the heirs by universal succession. The date of death is decisive for the scope of the estate and valuation of the inheritance assets.

Cryptocurrencies such as Bitcoin are considered to have an inheritable value.[51] They are part of the inheritance and are therefore transferable. Bitcoins that are recorded on a blockchain are attached to the latter. It is recommended to determine the heir of the cryptocurrency assets, thereby taking into account the value of these assets for calculating the recipient's share. Problems arise when the heir does not possess the necessary means (usually the private keys) to dispose of the inherited cryptocurrencies.

* * *

Endnotes

1. Federal Council Report – Legal framework for distributed ledger technology and blockchain in Switzerland, dated December 14, 2018 (https://www.newsd.admin.ch/newsd/message/attachments/55153.pdf).
2. *Cf.* https://www.admin.ch/gov/en/start/documentation/media-releases.msg-id-74420.html
3. *Cf.* https://www.fedlex.admin.ch/eli/fga/2020/16/de
4. *Cf.* FINMA ICO Guidelines, p. 2 *et seq*. https://www.finma.ch/en/news/2018/02/20180216-mm-ico-wegleitung
5. *Cf.* for example, p. 262 *et seq.*, p. 276 *et seq*. and p. 309 of the Dispatch.
6. Federal Council Explanatory Report – DLT-Draft Law, p. 8 https://www.newsd.admin.ch/newsd/message/attachments/56192.pdf; Zogg, *Bitcoin als Rechtsobjekt – eine zivilrechtliche Einordnung*, in: recht 2019, p. 95 *et seq*. and p. 242 *et seq*. of the Dispatch.
7. *Cf.* https://www.finma.ch/de/news/2019/09/20190911-mm-stable-coins
8. *Cf.* FINMA Supplement, p. 1; Houdrouge/Tenot, *Le droit suisse à l'heure de la technologie des registres électroniques distribués*, in: Not@lex 2020, pp 49–63, and p. 52.
9. The Swiss Federal Act on Currency and Payment Instruments determines Switzerland's legal tender. To date, only (i) coins issued by the federal government, (ii) banknotes issued by the Swiss National Bank, and (iii) Swiss franc sight deposits at the Swiss National Bank qualify as legal tender. Legal tender is considered "money" in the narrow sense and therefore an official means of payment.

10. *Cf.* Hauser-Spuehler/Meisser, *Eingenschaften der Kryptowährung Bitcoin*, in: digma 2018, p. 7; Müller/Reutlinger/Kaiser, *Entwicklungen in der Regulierung von virtuellen Währungen in der Schweiz und in der Europäischen Union*, in: EuZ 2018, p. 80.
11. https://www.snb.ch/en/mmr/speeches/id/ref_20190905_tjn/source/ref_20190905_tjn.en.pdf
12. *Cf.* https://www.snb.ch/de/mmr/reference/pre_20191008/source/pre_20191008.de.pdf
13. *Cf.* https://www.bis.org/publ/othp35.pdf; https://www.snb.ch/en/mmr/reference/pre_20201203/source/pre_20201203.en.pdf
14. https://www.snb.ch/en/mmr/reference/pre_20210610/source/pre_20210610.en.pdf
15. *Cf.* https://www.bis.org/publ/othp_mariana.pdf
16. *Cf.* https://www.bitcoinsuisse.com/news/canton-zug-accept-cryptocurrencies-for-tax-payment-in-2021; https://www.zg.ch/behoerden/finanzdirektion/direktionssekretariat/aktuell/kanton-zug-akzeptiert-ab-2021-kryptowaehrungen-fuer-steuerzahlungen
17. Kramer/Chabbey, Switzerland paves the way for tokenisation of securities and introduces new DLT trading platforms (retrievable under: https://www.iflr.com/article/b1tm398frpwpnq/switzerland-paves-the-way-for-tokenisation-of-securities-and-introduces-new-dlt-trading-platforms).
18. *Cf.* Kramer/Oser/Meier, *Tokenisierung von Finanzinstrumenten de lege ferenda*, in: Jusletter May 6, 2019, N 22; Dispatch, p. 107 *et seq*.
19. *Cf.* Dispatch, p. 277.
20. *Cf.* Federal Council Explanatory Report – DLT-Draft Law, p. 29; Dispatch, p. 277.
21. According to the DLT-Draft Law, DLT-Securities may also classify as securities; *cf.* Dispatch, p. 309.
22. *Cf.* Dispatch, p. 309.
23. It must be noted that this is a novel and rapidly developing field of law and different views can be taken as to the classification of crypto-assets as securities under Swiss law. In light of this, it cannot be excluded that FINMA will come to a different conclusion in the future, in particular with regard to cryptocurrencies. FINMA noted that they would reconsider their conclusion in light of the views taken in any future case law or any new legislation in this area.
24. *Cf.* FINMA ICO Guidelines, p. 4 *et seq*.
25. Federal Act on Financial Services of June 15, 2018, SR 950.1.
26. FINMA Supplement, p. 3.
27. FINMA Supplement, p. 4.
28. *Cf.* also Houdrouge/Tenot, *Le droit suisse à l'heure de la technologie des registres électroniques distribués*, in: Not@lex 2020, pp 49–63 and p. 53.
29. https://www.finma.ch/en/news/2021/09/20210929-mm-genehmigung-schweizer-kryptofonds
30. https://www.cryptofinance.ch/wp-content/uploads/2021/09/20210929_Crypto-Finance_Press_Release_Launch_Swiss_fund_EN.pdf
31. Federal Act on Financial Institutions of June 15, 2018, SR 954.1.
32. Federal Act on Financial Market Infrastructures and Market Conduct in Securities and Derivatives Trading of June 19, 2015, SR 958.1.
33. Federal Council Report – Legal framework for distributed ledger technology and blockchain, p. 122; Dispatch p. 309 *et seq*.
34. *Cf.* Swiss Legal Tech Association (SLTA), Regulatory Task Force Report, p. 33; the Federal Tax Administration publishes every year-end an exchange list (official exchange rate) for Bitcoin, Ethereum, Ripple, Bitcoin Cash, Litecoin, Cardano, NEM, Stellar, IOTA and Tron.

35. *Cf*. Swiss Legal Tech Association (SLTA), Regulatory Task Force Report, p. 34.
36. Federal Act on Anti-Money Laundering of October 10, 1997, SR 955.0.
37. *Cf.* FINMA ICO Guidelines, p. 6; FINMA Supplement, pp 2 and 7.
38. https://www.admin.ch/gov/en/start/documentation/media-releases.msg-id-64356.html
39. Federal Act on Banks of November 8, 1934, SR 952.0.
40. *Cf.* Arts 2 and 6 of the Swiss Banking Ordinance of April 30, 2014, SR 952.02.
41. *Cf.* Mueller/Reutlinger/Kaiser, p. 86 *et seq*.; Maurenbrecher/Meier, *Insolvenzrechtlicher Schutz der Nutzer virtueller Währungen*; Eggen, Chain of Contracts – *Eine privatrechtliche Auseinandersetzung mit Distributed Ledgers*, in: AJP 2017, p. 14; Bärtschi/Meisser, *Virtuelle Währungen aus finanzmarkt- und zivilrechtlicher Sicht*, in: Weber/Thouvenin (Hrsg.), *Rechtliche Herausforderungen durch webbasierte und mobile Zahlungssysteme*, Zurich 2015, p. 141.
42. *Cf*. Art. 1b of the Banking Act.
43. *Cf*. Art. 4^{sexies} of the Banking Act.
44. *Cf.* FINMA Supplement, p. 2.
45. *Cf*. FINMA Supplement, p. 2 *et seq*.
46. *Cf.* FINMA Supplement, p. 2 *et seq.*
47. *Cf.* FINMA Supplement, pp 2–4.
48. *Cf.* FINMA Supplement, p. 4.
49. Federal Council Report – Legal framework for distributed ledger technology and blockchain, p. 139.
50. Federal Council Report – Legal framework for distributed ledger technology and blockchain, p. 117.
51. *Cf*. Eigenmann/Fanti, *Successions, Données Personnelles, Numériques et Renseignements*, in: SJ 2017 II, p. 198.

* * *

Acknowledgment

The authors acknowledge with thanks the contributions of Schara Palan to this chapter.

Daniel Haeberli
Tel: +41 43 222 16 33 / Email: daniel.haeberli@homburger.ch

Daniel Haeberli is a banking and finance as well as a capital markets transactions and financial market regulations specialist. He is particularly focused on secured lending, syndicated debt and structured financing as well as derivatives, securitised structured products, investment funds and bond offerings. He regularly advises clients on blockchain projects and cryptocurrency matters.

Daniel Haeberli is the co-head of Homburger's "Technology and Digital Economy" practice group and he heads the "Legal & Regulation" working group of the Swiss Structured Products Association (SSPA).

Stefan Oesterhelt
Tel: +41 43 222 12 65 / Email: stefan.oesterhelt@homburger.ch

Stefan Oesterhelt's practice focuses on tax law, in particular international tax law, mergers and acquisitions, capital markets transactions and tax litigation. He is a lecturer on tax law at the University of Sankt Gallen and regularly speaks at seminars on tax law.

Alexander Wherlock
Tel: +41 43 222 17 50 / Email: alexander.wherlock@homburger.ch

Alexander Wherlock's practice focuses on financial markets and banking law. He regularly advises on banking regulation as well the regulation of derivatives markets and complex financial products. Alexander Wherlock is also a member of Homburger's "Technology and Digital Economy" practice group.

Homburger

Hardstrasse 201, 8005 Zurich, Switzerland
Tel: +41 43 222 10 00 / URL: www.homburger.ch

Taiwan

Robin Chang & Eddie Hsiung
Lee and Li, Attorneys-at-Law

Government attitude and definition

Cryptocurrencies, which are not linked or tied to the currency of any nation, are currently not accepted by the Central Bank of the Republic of China (Taiwan) ("CBC") as currency.

On 30 December 2013, both the CBC and Taiwan's Financial Supervisory Commission ("FSC") first expressed the government's position toward Bitcoin by issuing a joint press release ("2013 Release"). According to the 2013 Release, the two authorities held that Bitcoin should not be considered a "currency", but a highly speculative digital "virtual commodity". In another FSC press release in 2014 ("2014 Release"), the FSC ordered that local banks must not accept Bitcoin or provide any other services related to Bitcoin (such as the exchange of Bitcoins for fiat currency). On 4 July 2022, the FSC issued a letter to the local bankers association, requiring the association to forward the FSC's instruction prohibiting credit card acquirers from providing credit card services for purchase of crypto-assets in the Taiwan market, which is similar to the FSC's preceding position toward the online gambling, stocks, futures, options and other relevant transactions where the credit card service has been banned. Save for the letter, the FSC has not further officially promulgated any rules or regulations in relation to proposed new requirements as of the date of writing. The FSC further issued press releases on 19 December 2017 ("2017 Release") and 4 March 2022, in which the FSC reiterated the government's position as specified in the 2013 and 2014 Releases.

Other than the above, no laws, regulations or rulings have been officially issued, promulgated or amended to specifically deal with the rise of cryptocurrencies, except for the regulations governing the offering and issuance of any tokens with the nature of securities (which are commonly called "security tokens", and their offering commonly called "security token offerings" ("STOs")) as discussed under "Sales regulation" below.

Cryptocurrency regulation

Please see "Government attitude and definition" above. So far, except for the STO regulations discussed under "Sales regulation" below, no Taiwanese laws or regulations have been promulgated or amended to formally regulate "virtual currencies" or "cryptocurrencies"; therefore, virtual currencies/cryptocurrencies cannot currently be considered "legal tender", "currencies" or a generally accepted "medium of exchange" in Taiwan.

Further, there currently exists no required licence in Taiwan for (a) operating the services of exchange between virtual currencies or virtual currencies with fiat currencies, or (b) acting as a "money transmitter" and the like in Taiwan.

Sales regulation

Sale of Bitcoins or any other virtual currencies/cryptocurrencies of the same nature and characteristics

So far, except for the STO regulations discussed below, there exist no laws or regulations specifically dealing with the sale of virtual currencies/cryptocurrencies. The sale of Bitcoins, currently considered by the FSC as a sale of a digital "virtual commodity" but not "currency", should generally be fine from a Taiwan regulatory perspective, and the general principles and rules governing "purchase and sale" under the Civil Code would apply if the consideration were cash. Also, we tend to think that the above would apply to the sale of other virtual currencies/cryptocurrencies of the same nature and characteristics as Bitcoin.

Please note that the above is subject to "ICO and token offering" as described below.

ICO and token offering

In response to the rising amount of initial coin offerings ("ICOs") and other investment activities regarding virtual currencies/cryptocurrencies, the FSC also expressed the following view on ICOs through the 2017 Release as mentioned above:

(1) An ICO refers to the issue and sale of "virtual commodities" (such as digital interests, digital assets, or digital virtual currencies) to investors. The classification of an ICO should be determined on a case-by-case basis. For example, if an ICO involves the offer and issue of "securities", it should be subject to Taiwan's Securities and Exchange Act ("SEA"). The issue of whether tokens in an ICO would be deemed "securities" under the SEA would depend on the facts of each individual case.
(2) If any misrepresentations with respect to technologies or their outcomes, and/or promises of unreasonably high returns, are used by the issuer of virtual currencies or an ICO to attract investors, the issuer would be deemed to be committing fraud or illegal fundraising.

Given the above, in an ICO (or other type of token offering, such as private token pre-sale before the ICO stage), the core issue in this regard is whether an ICO would be considered an issuing of "securities" under Taiwan's securities regulations. Under current Taiwan law, the offer and sale of "securities" in Taiwan, whether through public offering or private placement, are regulated activities and shall be governed in accordance with the SEA and its related regulations as well as relevant rulings issued from time to time by the FSC.

Security tokens and STOs

On 3 July 2019, the FSC, by issuing a ruling, officially designated cryptocurrencies with the nature of securities, i.e., security tokens, as "securities" under the SEA ("2019 Ruling"). According to the 2019 Ruling, security tokens refer to those that:

- utilise cryptography, distributed ledger technology or other similar technologies to represent their value that can be stored, exchanged or transferred through a digital mechanism;
- are transferable; and
- encompass all of the following attributes of an investment:
  - funding provided by investors;
  - providing funding for a common enterprise or project;
  - investors expecting to receive profits; and
  - profits generated primarily from the efforts of the issuer or third parties.

In addition to the 2019 Ruling, the FSC issued a press release on 27 June 2019 to illustrate the key points of the FSC's policy on STOs. Since then, the FSC and the Taipei Exchange ("TPEx") have been setting out the set of regulations governing STOs, and the

STO regulations were finalised in January 2020. Specifically, the FSC differentiates the regulation of STOs with the threshold of 30 million New Taiwan Dollars ("NT$"). For an STO of NT$30 million or less, the STO may be conducted in compliance with the STO regulations; an STO above NT$30 million must first apply to be tested in the "financial regulatory sandbox" pursuant to the Sandbox Act and, in case the experiment has a positive outcome, should be conducted pursuant to the SEA. Please see the below summary of certain key provisions of the STO regulations (i.e., for STOs of NT$30 million or less):

- Qualifications of the issuer – the issuer must be a company limited by shares incorporated under the laws of Taiwan and not a company listed on the Taiwan Stock Exchange or TPEx or traded on the Emerging Stock Market.
- Types of security tokens that can be issued – the issuer can only issue profit-sharing or debt tokens without shareholders' rights.
- Eligible investors and amount limits – currently, only "professional investors" are eligible to participate in STOs; where the professional investor is a natural person, the maximum subscription amount is NT$300,000 per STO.

STO platform operator

- Qualifications of the platform operator – the platform operator should obtain a securities dealer licence, have a minimum paid-in capital of NT$100 million and provide an operation bond in the amount of NT$10 million.
- Total offering amount capacity – the total offering amount of all STOs on a single platform should not exceed NT$200 million. A platform can accept to process a second STO only six months after the security tokens of the first STO have been traded on the platform.
- Transfer and record-keeping – the platform operator should enter into an agreement with the Taiwan Depository and Clearing Corporation ("TDCC") and transmit the trading information, such as balance changes and a balance statement, to the TDCC for its record on a daily basis. The TDCC should provide an STO balance inquiry service to investors.

Pursuant to the STO regulations, there are also some other requirements and restrictions including those regarding trading (secondary market), real-name basis, NT$ only, etc.

Taxation

There is currently no regulation specifically governing the taxation of cryptocurrencies; however, by referring to the tax laws and tax rulings in connection with the taxation of cross-border e-commerce transactions and online sales of services, it is possible that the tax authorities might take the following stances.

Business tax (also known as value-added tax or "VAT")

The trading of cryptocurrencies on a platform within Taiwan may be deemed a sale of services within Taiwan and thus be subject to Taiwan business tax as follows:

(i) If the seller is a Taiwan business entity, the seller will be subject to 5% VAT on the revenue.
(ii) If the seller is a Taiwanese individual, the individual should apply for tax registration and pay 5% VAT on the revenue, unless the monthly sales amount is under NT$40,000 (approx. US$1,300).
(iii) If the seller is a foreign entity with a fixed place of business in Taiwan (e.g., a Taiwan branch), the Taiwan branch should pay 5% VAT on such revenue.
(iv) If the seller is a foreign entity without a fixed place of business in Taiwan, and the purchasers of the cryptocurrencies are entirely Taiwanese entities, the seller will have no business tax issue; instead, the purchasers will become the taxpayer.

(v) If the seller is a foreign entity without a fixed place of business in Taiwan, and the purchasers of the cryptocurrencies include Taiwanese individuals, the foreign seller should apply for tax registration and pay 5% VAT on the revenue generated from the sale of the cryptocurrencies to the Taiwanese individuals, unless the monthly sales amount to the Taiwanese individuals is under NT$40,000 (approx. US$1,300).

Income tax

Any income generated from the trading of cryptocurrencies on an onshore platform ("Trading Income") may be deemed income sourced from Taiwan and thus be subject to Taiwan income tax as follows:

(i) If the seller is a Taiwan business entity, the seller should consolidate the Trading Income into its other taxable income for calculating its Taiwan income tax payable. (The prevailing income tax rate is generally 20% on the net taxable income.)
(ii) If the seller is a Taiwanese individual, the individual should consolidate the Trading Income into its other taxable income for calculating its Taiwan income tax payable. (The prevailing highest progressive tax rate is 40% on the net taxable income.)
(iii) If the seller is a foreign entity with a fixed place of business in Taiwan (e.g., a Taiwan branch), the Taiwan branch should consolidate the Trading Income into its other taxable income and pay income tax accordingly. (The prevailing income tax rate is generally 20% on the net taxable income.)
(iv) If the seller is a foreign entity with a business agent in Taiwan, the business agent should, on behalf of the foreign entity, file an income tax return, report the Trading Income, and pay income tax accordingly. (The prevailing income tax rate is generally 20% on the net taxable income.)
(v) If the seller is a foreign entity without a fixed place of business or business agent in Taiwan, the seller should file an income tax return (the seller may engage a tax agent to file the tax return on its behalf), report the Trading Income, and pay income tax accordingly. (The prevailing income tax rate is generally 20% on the net taxable income.)

Money transmission laws and anti-money laundering requirements

As advised under "Cryptocurrency regulation" above, there currently exists no required licence for (a) operating the services of exchange between virtual currencies or virtual currencies with fiat currencies, or (b) acting as a "money transmitter" and the like in Taiwan.

As for anti-money laundering, the latest amended Money Laundering Control Act of Taiwan ("Taiwan AML Act"), which took effect on 7 November 2018, has brought cryptocurrency platform operators into the anti-money laundering regulatory regime, under which the enterprises falling within the designated scope will be subject to the relevant rules applicable to financial institutions under the Taiwan AML Act. On 7 April 2021, Taiwan's Executive Yuan issued a ruling ("AML Ruling"), interpreting the scope of enterprises of "virtual currency platforms and trading business" under the Taiwan AML Act. The scope described under the AML Ruling covers those who engage in the following activities for others:

(1) Exchange between virtual currency and NT$, foreign currencies or currencies issued by Mainland China, Hong Kong or Macao.
(2) Exchange between virtual currencies.
(3) Transfer of virtual currencies.
(4) Custody and/or administration of virtual currency or providing instruments enabling control over virtual currencies.
(5) Participation in and provision of financial services related to the issuance or sale of virtual currencies.

After the AML Ruling was issued, the FSC further published the Regulations Governing Anti-Money Laundering and Countering the Financing of Terrorism for Enterprises of Virtual Currency Platforms and Trading Business. According to such regulations, the designated operators of crypto-assets and exchanges are required to establish, among others, an internal control and audit mechanism, a reporting procedure of suspicious transactions, and the know-your-customer procedure, etc. The regulations took effect from 1 July 2021 other than the provision requiring the "transfer out" of the cryptocurrency to be carried out on a real-name basis both for the transferor and transferee – the effective date of such provision will be further determined and announced by the FSC.

Please also note that the FSC, however, issued a press release on 30 March 2023 stating that it will serve as the competent authority for virtual asset platforms of a financial investment or payment nature, and will, under the Taiwan AML Act, establish nine guiding principles, which include information disclosure of virtual asset platforms, product launch and discontinuation review, separate custody of customer and platform assets, fair and transparent transactions, anti-money laundering, protection of customer rights, information security, operating systems, hot and cold wallet management and institution review, to strengthen industry self-discipline and information disclosure before the end of the third quarter of 2023. It would be prudent for industry players to pay attention to the potential regulatory developments in Taiwan.

Promotion and testing

Taiwan's law for the fintech regulatory sandbox, the "FinTech Development and Innovation and Experiment Act" ("Sandbox Act"), was promulgated on 31 January 2018 and took effect on 30 April 2018. The Sandbox Act was enacted to enable fintech businesses to test their financial technologies.

According to the Sandbox Act, an applicant (which can be an entity or individual) needs to obtain approval from the FSC before entering the sandbox. Once the experiment begins, the experimental activities may enjoy exemptions from certain laws and regulations (such as FSC licensing requirements and certain legal liability exemptions).

After completion of the approved experiments, the FSC will analyse the results of the experiments. If the result is positive, the FSC will actively examine the existing financial laws and regulations to explore the possibility of amending them, after which the business model or activities previously tested in the sandbox could become feasible under law. Please note, however, that the sandbox entity or individual might still be required to apply for a relevant licence or approval from the FSC in order to formally conduct the activities as previously tested in the sandbox.

At the time of writing, none of them are related to cryptocurrencies. Nonetheless, please note that under the STO regulations as advised above, there would be an upper limit for the total amount of an STO programme, and according to relevant news reports, the FSC mentioned that any STO exceeding such upper limit may first need to be tested and experimented with in the regulatory sandbox.

Even so, it is possible that the relevant STO market players, as well as some controversial fintech business models and activities (e.g., ICOs), would wish to apply to the FSC to enter the sandbox. However, according to the Sandbox Act, any experimental activity needs to be "innovative". Therefore, (a) whether or not commonly seen cryptocurrency-related activities (such as ICOs and/or STOs) would enter the sandbox, and (b) if yes, whether the result of the experiment would be considered "positive", would still depend on the FSC's then-effective policies and final decision.

Ownership and licensing requirements

As mentioned above, except for the STO regulations advised above, Taiwan has not promulgated any laws or regulations specifically dealing with "virtual currencies" or "cryptocurrencies". Therefore, there exist no ownership or licensing requirements under Taiwanese law, except for the STO platform operator (which should obtain a securities dealer licence) as advised under "Sales regulation" above.

Mining

So far, no Taiwanese laws or regulations have been promulgated or amended to regulate the "mining" of Bitcoin or any other types of cryptocurrency. Mining activities are generally permitted.

Border restrictions and declaration

So far, no Taiwanese laws or regulations have been specifically promulgated or amended to impose any border restrictions on, or requirements for, declaration of holdings of cryptocurrencies.

Reporting requirements

So far, save for the reporting obligations under the STO regulations as well as cryptocurrency platform operators' reporting obligations in relation to the suspicious transactions for anti-money laundering purposes as mentioned above, no Taiwanese laws or regulations have been specifically promulgated or amended to impose any reporting requirements for cryptocurrencies.

Estate planning and testamentary succession

So far, Taiwan's laws and regulations have not addressed this topic. Since cryptocurrencies have value, we tend to think they would be considered "property" or "assets" from the perspective of Taiwan estate and succession law, unless they are confiscated by the government due to, for example, the commission of a criminal offence violating the prohibition of "securities" offerings without prior approval from, or registration with, the FSC as required under the SEA (see our advice under "Sales regulation" above).

Robin Chang
Tel: +886 2 2763 8000 ext. 2208 / Email: robinchang@leeandli.com

Mr. Robin Chang is a partner at Lee and Li and the head of the firm's banking practice group. His practice focuses on banking, IPOs, capital markets, M&A, project financing, financial consumer protection law, personal data protection law, securitisation and antitrust law.

Mr. Chang advises major international commercial banks and investment banks on their operations in Taiwan, including providing advice on compliance and regulatory issues, setting up a banking branch or bank subsidiary in Taiwan and customer complaints. He has been involved in many M&A transactions of financial institutions. He has also been involved in government projects in e-payment regulations in Taiwan.

Eddie Hsiung
Tel: +886 2 2763 8000 ext. 2162 / Email: eddiehsiung@leeandli.com

Mr. Eddie Hsiung is a partner at Lee and Li. He is licensed to practise law in Taiwan and New York, and is also a CPA in Washington State, U.S.A. His practice focuses on securities, M&A, banking, finance, asset and fund management, cross-border investments, general corporate and commercial, fintech, startups, etc. He regularly advises leading banks, securities firms, payment and credit card and other financial services companies on transactional, licensing and regulatory and compliance matters, as well as internal investigations. He is familiar with legal issues regarding the application of new technologies such as fintech (e-payment, digital financial services, and regulatory sandboxes), blockchain (ICOs, cryptocurrencies, platform operators) and AI, and is often invited to participate in public hearings, seminars and panel discussions in these areas.

Lee and Li, Attorneys-at-Law

8F, No. 555, Sec. 4, Zhongxiao East Road, Taipei 11072, Taiwan, R.O.C.
Tel: +886 2 2763 8000 / URL: www.leeandli.com

Thailand

Jason Corbett & Don Sornumpol
Silk Legal Co., Ltd.

Government attitude and definition

Based on its current policies, the Thai government is generally supportive of cryptocurrency since it diversifies the means through which Thai business operators may raise investment capital, and since the technology may be used to contribute to national development. Nevertheless, the government is also wary of the effect of cryptocurrency on the nation's financial stability, its economic system, and the wider public.

In consultation with the Bank of Thailand and a public hearing between 25 January to 8 February 2022, the Securities and Exchange Commission of Thailand (the "SEC"), which regulates cryptocurrencies and other digital assets in Thailand, has issued a directive effective 1 April 2022 concerning the use of cryptocurrency as a means of payment. The directive prohibits "digital asset business operators" (discussed herein) from allowing cryptocurrency to be used as a means of payment for goods and services. In summary:

(1) digital asset business operators are prohibited from providing any service or engaging in any activity that supports or promotes using cryptocurrency as a means of payment, such as advertising, solicitation, or indicating that it is willing to offer its services to assist in using cryptocurrency as a means of payment, etc.; and
(2) any digital asset business operator who discovers a customer using their account for a purpose relating to payments for goods and services must warn such customers that their use of the services of the digital asset business violates the terms of use, and must take action against such customers where appropriate, including the suspension of such accounts.

The Bank of Thailand and a consortium of Thai commercial banks have been engaged in a research and development project called Project Inthanon, which relates to the development of a central bank digital currency ("CBDC"). Project Inthanon was initiated in 2019 and has been through two phases relating to a wholesale CBDC, including one phase that was conducted in conjunction with the Hong Kong Monetary Authority concerning cross-border payments. The testing of the retail CBDC is expected to proceed in late 2022.

Cryptocurrency regulation

Digital assets, which include cryptocurrencies, are regulated by the Emergency Decree on Digital Asset Businesses B.E. 2561 (2018) (the "Emergency Decree") and a series of regulations issued by the Ministry of Finance and the SEC. There is no general prohibition against cryptocurrencies.

Sales regulation

The sale of Bitcoin or other tokens to the public is regulated by its specific legislation, which is the abovementioned Emergency Decree and is not directly regulated by general securities and commodities laws. The Emergency Decree regulates both secondary trading in cryptocurrency and "initial coin offerings" ("ICOs").

Regarding secondary trading, selling cryptocurrency to the public requires one to be licensed as a "digital asset business operator" under the Emergency Decree in the form of one of the following:

(1) Digital Asset Exchange: "[A] center or a network established for the purposes of trading or exchanging of digital assets, which operates by matching orders or arranging for the counterparty or providing the system or facilitating a person who wishes to trade or exchange digital assets to be able to enter into an agreement or match the order, in the normal course of business, excluding the center or network in the manner as specified in the notification of the SEC."

(2) Digital Asset Broker: "[A] person who provides services or holds itself out to the public as available to provide services as a broker or an agent for any person with respect to the trading or exchange of digital assets in the normal course of business, in consideration of a fee or other remuneration, excluding the brokers or agents who act in the manner as specified in the notification of the SEC."

(3) Digital Asset Dealer: "[A] person who provides services or holds itself out to the public as available to provide services with respect to the trading or exchange of digital assets for its own account in the normal course of business outside the digital asset exchange, excluding the dealers who act in the manner as specified in the notification of the SEC."

Regarding ICOs, the Emergency Decree generally requires that an offeror must obtain approval from the SEC and file a registration statement similar to what is required for a traditional offering of securities. Furthermore, the ICO must be offered through a "Digital Portal Service Provider" who has been approved by the SEC. Additionally, a comprehensive regulation applicable to ICOs is detailed in SEC Notification No. 15/2561 issued on 3 July 2018. This regulatory framework divides digital tokens into "investment tokens", defined as digital tokens that define the rights of investors in a particular project or activity, and "utility tokens", which define rights to receive goods and services. The ICO regulations apply to issuances of investment tokens and only utility tokens that are not ready to be utilised from the date of issuance. Utility tokens that are ready to be utilised from the date of issuance are expressly exempt from ICO regulations by SEC Notification No. 10/2561 issued on 7 June 2018.

Taxation

The Revenue Code classifies income derived from cryptocurrency or digital tokens as taxable income as follows: "(h) share of profits or other benefit of the same character that is derived from holding or possessing cryptocurrency, (i) a benefit derived from transferring cryptocurrency or digital tokens where the monetary value exceeds the investment..." (Section 40(4)(h)(i)). Additionally, where cryptocurrency or digital assets are paid as income, the applicable withholding tax rate is 15% (Section 50(2)(f)).

The transfer of cryptocurrency or digital tokens that occurs in a digital asset exchange (licensed by the Ministry of Finance) is exempt from value-added tax (Emergency Decree No. 744), as is the transfer of digital currency developed and issued by the Bank of Thailand to the public between 1 April 2022 to 31 December 2023 (Emergency Decree No. 745).

Furthermore, on 7 March 2023, the Cabinet approved a draft Emergency Decree that will exempt corporate income tax and value-added tax for juristic entities that issue and sell investment tokens to the public under the Emergency Decree on Digital Asset Businesses B.E. 2561. It will also exempt value-added tax on the sale of investment tokens that occur from 14 May 2018 onwards, regardless of whether or not the sale occurs within a digital asset exchange licensed by the Ministry of Finance. This draft Emergency Decree is subject to publication in the Royal Gazette.

Money transmission laws and anti-money laundering requirements

For the Anti-Money Laundering Act B.E. 2542 (1999), which is the general anti-money laundering legislation in Thailand, Section 7 of the Emergency Decree classifies both digital asset business operators and digital token portal service providers as "financial institutions". Therefore, any anti-money laundering requirements that would normally apply to financial institutions are equally applicable to the aforementioned digital asset businesses. Generally, the Anti-Money Laundering Act requires financial institutions to report suspicious transactions and screen customers, among other requirements.

Money transmission in Thailand is covered under the Payment System Act B.E. 2560 (2017). However, this legislation does not subject the transmission of digital assets or cryptocurrency to regulation. Furthermore, as discussed above, digital asset business operators are prohibited from encouraging or assisting in making cryptocurrency or digital assets a means of payment for goods and services.

Promotion and testing

On 4 June 2021, the Bank of Thailand published guidelines on the use of blockchain technology by financial service providers. Such guidance is offered in conjunction with the regulatory sandbox programme offered by the Bank of Thailand, which allows financial service providers an opportunity to test and develop innovative technology that is to be used in delivering their services. Therefore, it is evident that the policy of the Bank of Thailand is to promote research and development into blockchain technology by the private sector.

Ownership and licensing requirements

The Ministry of Finance issued a notification on 19 October 2020 that classified "digital asset fund managers" and "digital asset advisors" as digital asset business operators subject to licensing requirements. A later notification on 13 July 2022 further added the category of "digital asset custodial service providers". The notification defines these categories as follows:

(1) Digital Asset Fund Manager: "[A] person who provides services or holds itself out to the public as available to provide services with respect to managing funds on account of others in the normal course of business, excluding managers who act in the manner as specified in the notification of the SEC."
(2) Digital Asset Advisor: "[A] person who offers recommendations to the public whether directly or indirectly relating to the value of digital assets, or the suitability of investing in digital assets, or buying, selling, or exchanging any digital assets in the normal course of business, in exchange for a fee or other consideration, excluding advisors who act in the manner specified in notification of the SEC."
(3) Digital Asset Custodial Service Provider: "[A] person who provides services or holds itself out to the public as available to provide services, in any manner, which is done in the normal course of business, in exchange for a fee or other consideration as follows:

(a) accepting deposit or safekeeping of digital assets;
(b) management of a cryptographic key or any other thing that must be kept confidential that is necessary to allow a transfer or transaction related to digital assets, whether authorization is general or limited.

The services described above do not include any service that is included within the scope of acting as a digital asset exchange, digital asset broker, digital asset dealer, or digital asset fund manager, or any service in the manner as specified in the notification of the SEC."

Mining

On 7 January 2022, the Revenue Department issued a statement clarifying that, in their view, Bitcoin mining is analogous to a manufacturing operation and is therefore taxable under Section 40(8) of the Revenue Code. The aforementioned section refers to "income from business, commerce, agriculture, industry, transport or any other activity" not specified in the other categories under Section 40(4). The miner would be taxed on the profit earned after deducting the cost of setting up the operation, i.e. the cost of the computers, graphics cards, building, air conditioning, etc. from the value of the Bitcoin mined through the operation. The purpose of this announcement was to close a loophole, since the current Revenue Code under Section 40(4) only taxes income derived from cryptocurrency or digital assets when they are traded (source: https://www.matichon.co.th/economy/news_3121083 (Thai language)).

Border restrictions and declaration

There are no obligations to declare cryptocurrency holdings when entering or exiting the country or in general. However, where a digital asset operator will provide services to a client related to investment in digital assets that are traded in a foreign country, the SEC places some restrictions on the digital asset operator: The digital assets must be those that are lawfully traded in the foreign country that is the target of investment, and the foreign country should be a member of the International Organization of Securities Commissions ("IOSCO") and a Signatory to the Multilateral Memorandum of Understanding Concerning Consultation and Cooperation and the Exchange of Information ("MMOU"). Furthermore, when investing in a foreign-based ICO, such ICO must not be conducted in a manner evidencing an intention to offer the token in Thailand. Furthermore, there are additional guidelines to follow where the client participating in the ICO is a retail investor. SEC Notification No. 3/2561 (11 July 2018).

Reporting requirements

As mentioned above, digital asset business operators are classified as "financial institutions" for anti-money laundering legislation. According to the Anti-Money Laundering Act and Ministerial Regulations, financial institutions are required to report any cash transaction from THB 2,000,000 or more to the Anti-Money Laundering Office.

Estate planning and testamentary succession

Cryptocurrencies and other digital assets are considered "property" for the purposes of Section 138 of the Civil and Commercial Code and would be included in an owner's estate upon death. However, the enforcement of court judgments in civil matters, including judgments probating wills and settling intestacy issues, is within the responsibility of the

Legal Execution Department (the "LED") under the Ministry of Justice. According to press releases and research reports published in recent years, the LED has shown great interest in studying the issue of how to enforce court judgments related to cryptocurrency and digital assets in general. The LED has also been extensively studying how the issue is treated under legal systems of other jurisdictions in this regard, including Canada, Japan and the United States for purposes of comparison (source: https://www.led.go.th/articles/pdf/uO5ivavpioXiwe0zVD7ZS4DVtO0m3M27shbWXJzP2933110119024416.pdf (Thai language)). Furthermore, the Royal Decree Exempting Certain Transactions in the Civil and Commercial Code from the Electronic Transaction Act of B.E. 2548 (2005) exempts testamentary transactions from coverage under the Electronic Transaction Act of B.E. 2544 (2001). As a result, electronic evidence cannot be admitted in court for the purpose of probating an estate. Therefore, such a restriction could pose as a serious obstacle to trying to affect a testamentary disposition of digital assets.

Jason Corbett
Tel: +66 2 107 2007, Ext. 310 / Email: jason@silklegal.com

Dr. Jason Corbett is the founder and Managing Partner of Silk Legal and has advised clients on a variety of matters, including cross-border insolvency and restructuring, mergers and acquisitions, commercial transactions, fintech, and blockchain.

Jason's interest and proficiency in matters of technology and innovation have made him a leader in providing cutting-edge solutions to solve the challenges found in the practice. His notable competencies in this area have allowed him to assist investors, managers, and other stakeholders tackle a variety of legal, business, and intellectual property issues.

Moreover, with over 15 years of experience as an insolvency specialist, he has also assisted shareholders, creditors, receivers, trustees, and many others in successfully concluding insolvency proceedings. His work has made him adept at formulating and executing out-of-court settlements that have bested interjurisdictional complexities. As the Thailand member of the International Insolvency Institute, he is considered one of the most sought-after legal counsel for creditors seeking to protect their interests in Thailand.

Don Sornumpol
Tel: +66 2 107 2007, Ext. 311 / Email: don@silklegal.com

Since 2012, Don Sornumpol has handled matters that span across multiple practice areas, including corporate and commercial, fintech, and real estate law. During his tenure as an experienced attorney, he has represented several prolific companies.

Don's previous experience includes leading due diligence and evaluation projects, as well as drafting and reviewing purchasing, structuring, licensing, and financing agreements. He is highly skilled in legal research and advising clients on new laws and regulations, including privacy and data protection, fintech, and cybersecurity. He also has significant experience in dealing with small and medium enterprises (SMEs), in addition to larger corporations.

Don also heads Silk Legal LLP in New York City (USA), which serves the firm's clients who work in the fields of blockchain and digital assets.

Silk Legal Co., Ltd.

RSU Tower, 8th Floor Suite 805, 571 Sukhumvit Road (Soi 31), North Klongton, Watthana,
Bangkok, 10110, Thailand
Tel: +66 2 107 2007 / URL: www.silklegal.com

Turkey/Türkiye

Alper Onar & Emre Subaşı
Aksan Law Firm

Government attitude and definition

Government attitude towards crypto assets

Türkiye is one of the largest[1] and fastest crypto adopters globally. It was estimated that over 5 million[2] people currently own cryptocurrency in Türkiye according to the Crypto Currency Research Report published by the Information Technologies and Communication Authority of Türkiye in May 2020. Currently, there is no legal investor protection scheme for crypto assets. However, the government is working on an Unofficial Draft Legislation on crypto assets and crypto asset service providers ("**Unofficial Draft Legislation**")[3] amending Capital Markets Law No. 6362 ("**CML**"). Although there is no official press release regarding the timeline of the Unofficial Draft Legislation, it is expected to be submitted to the Grand National Assembly of Türkiye within the short term and will impose additional requirements for crypto asset service providers ("**CASPs**") operating in Türkiye.

In general, the Unofficial Draft Legislation aims to regulate crypto assets, crypto asset trading platforms, crypto wallets, crypto asset custody services and CASPs in Turkish legislation for the first time.

Please note that, at the time of writing, crypto assets are not qualified as "capital markets instruments" but defined as "*an intangible asset representing a value or right that can be created and stored virtually through distributed ledger technology or any other similar technology and that can be distributed over digital networks*" in the Regulation Prohibiting Payments Through Crypto Assets, which was issued by the Central Bank of the Republic of Türkiye and entered into force on April 30th, 2021 ("**Central Bank Regulation**"). This definition distinguishes crypto assets from capital markets instruments, making them subject to a different legal regime.

CASPs will be subject to a licence to be issued by the Capital Markets Board of Türkiye ("**CMB**") for their foundation and operation and these trading platforms will be subject to the supervision of the CMB for their compliance with the relevant CML regulations.

The main expected principles of the Unofficial Draft Legislation are provided below:

- CASPs are obliged to obtain operating licences issued by the CMB.
- CASPs are defined as "*crypto asset exchange platforms, crypto asset custodians and any other service provider providing services in relation to crypto assets*".
- The CMB will be authorised to issue secondary legislation in relation to many issues ranging from the operation principles of CASPs to the designation of crypto assets to be traded on the CASPs and to decide on their termination and disposal. Additionally, certain securities determined by the CMB can be issued directly as a crypto asset.

- After the enactment of the Unofficial Draft Legislation, the CMB will impose certain restrictions not only for unauthorised CASPs' activities but also for the solicitation to Turkish residents by unauthorised CASPs.
- Likewise, individuals and institutions (including, but not limited to, investment managers, investment advisors or fund managers and CASPs) that will be operating in the crypto asset industry without obtaining a licence or permission from the CMB would face criminal consequences due to unauthorised capital market activity.
- CASPs will be subject to the supervision of the CMB in terms of compliance with the relevant CML provisions.
- Crypto asset holders may enjoy the right to self-custody of their crypto assets. They may also store their crypto assets at banks that are deemed appropriate by the Banking Regulatory and Supervisory Authority ("**BRSA**"), or crypto asset custodians licensed by the CMB.
- TÜBİTAK (the Scientific and Technological Research Council of Türkiye) will be authorised to evaluate the technicalities of crypto assets.
- Similar to the directors of intermediary service providers, the directors of CASPs will also be subject to conditions set forth in the CML and the relevant *communiqués*.
- Framework agreements between customers and CASPs, which need to be written and can be concluded by means of online communication, will be governed by the CMB's secondary regulation.

Except for transactions related to crypto assets that are also traded in foreign markets and whose prices are also formed in foreign markets, an activity that cannot be explained with a reasonable and economic justification and that may disrupt the safe and stable operation of transactions on a CASP may be deemed market abuse according to the Unofficial Draft Legislation Investor Compensation Scheme under Article 83 of the CML.

Moreover, while restricting new entries to the Turkish market without obtaining an operating licence, it is expected that the Unofficial Draft Legislation will provide an interim transition period, known as "grandfathering", for CASPs that are active and already incorporated in Türkiye to pursue their activities until the secondary legislation is enacted. Unauthorised activities will be subject to sanctions provided in the CML.

Even though the first drafts of Unofficial Draft Legislation provided a closed environment for "un-hosted wallets", this approach was strongly criticised. Therefore, the latest Unofficial Draft Legislation abandons the restrictive approach and allows citizens to freely transfer crypto assets from CASPs to "un-hosted wallets" in line with the anti-money laundering ("**AML**") and counter-terrorist financing ("**CTF**") approaches of the Financial Action Task Force ("**FATF**").

Finally, considering the recent developments in the European Union ("**EU**") regarding the conclusion of the trialogues between the Council and the European Parliament on Markets in Crypto-Assets ("**MiCA**") and its publication in the Official Journal of the European Union, it is observed that the Unofficial Draft Legislation does not provide a strict regulatory approach but constitutes a regulatory framework for future secondary pieces of legislation. In this vein, upon the entry into force of the Unofficial Draft Legislation or its amended version, it can be safely assumed that the CMB will seek to implement secondary pieces of legislation to reach regulatory harmonisation with the EU.

Definition of crypto assets in Central Bank Regulation

Currently, the Central Bank Regulation is the first and only regulation defining and directly governing cryptocurrencies. The Central Bank Regulation refers to cryptocurrencies as "crypto assets" and defines crypto assets as "*intangible assets that are created virtually*

using distributed ledger or similar technologies and are distributed over digital networks, and that are not qualified as money, registered money, electronic money, payment instrument, security, or any other capital markets instrument". The reasoning behind the Central Bank Regulation is explained with several factors, as follows: (1) the use of crypto assets in payments may cause non-recoverable losses for the parties to the transactions due to a lack of regulation and supervision mechanisms for these assets and the probability of excess volatility; (2) there is no guaranteed mechanism to provide security for wallets; and (3) they may be used in illegal acts due to their anonymous structures.

Even though the purpose of the Central Bank Regulation is mainly to determine procedures and principles regarding the prohibition of the use of crypto assets in payments, the Central Bank Regulation can still be considered groundbreaking as it provides a definition of "crypto assets" for the first time in Türkiye.

Article 3.2 of the Central Bank Regulation explicitly prohibits any type of direct or indirect payment by means of crypto assets, followed by Article 3.3, which prohibits providing services for the use of crypto assets, directly or indirectly, in payments.

Furthermore, Articles 4.1 and 4.2 of the Central Bank Regulation provide that payment service providers (banks, payment companies, e-money companies) are not authorised to:

- cooperate or build business models enabling the use of crypto assets, directly or indirectly; or
- provide any services to such business models to use crypto assets, directly or indirectly, in payment services or issuance of e-money.

Since the Central Bank Regulation's prohibition only refers to payments, collaborating with CASPs remains possible for banks in Türkiye to provide the integration services for customer accounts to facilitate fiat-to-crypto and/or crypto-to-crypto transactions.

It is clear that the Central Bank Regulation in Türkiye introduced a strict restriction on payments in crypto assets and the use of crypto assets by payment service providers. However, some parties are expecting a more flexible approach with the upcoming legislation on crypto assets.

Furthermore, crypto assets are neither treated as money nor equated to fiat currency under Turkish law. However, it is essential to assess whether crypto assets are treated as "e-money". The Law on Payment and Securities Settlement Systems, Payment Services and Electronic Money Institutions No. 6493 ("**Law No. 6493**") defines e-money as "*monetary value that is issued on the receipt of funds by an electronic money issuer, stored electronically, used to make payment transactions defined in Law No. 6493 and also accepted as a payment instrument by natural and legal persons other than the electronic money issuer*". In addition, the BRSA implicitly excludes[4] Bitcoin when defining "e-money".

Crypto assets whose prices are pegged to the value of fiat currency or any other external reference are known as "stablecoins". Arguably, in the event that a stablecoin issuer fulfils the criteria set forth in Law No. 6493 and other applicable regulations, there might be a theoretical possibility that the issued (so-called) stablecoin can be treated as "e-money". However, as explained above, the Central Bank Regulation strictly prohibits payments with crypto assets. Therefore, currently, it could be safe to say that crypto assets are neither treated as "money" nor "e-money".

Taking into account the disasters in the stablecoin ecosystem (such as the Terra/Luna collapse) and recent developments on the regulatory framework of stablecoins to protect

investors and preserve financial stability (such as the MiCA), additional legal developments on these issues in Türkiye can be expected prior to the entry into force of the relevant articles of the MiCA concerning asset-referenced tokens and e-money tokens.

Government and the central bank

There is no regulation concerning government-/central bank-backed crypto assets. However, in a press release numbered 2021/40 of September 15th, 2021,[5] the Central Bank of the Republic of Türkiye announced that it had signed bilateral memorandums of understanding with ASELSAN,[6] HAVELSAN[7] and TÜBİTAK-BİLGEM (the Informatics and Information Security Research Center) and established the "Digital Turkish Lira Collaboration Platform", and plans to carry out tests that may diversify the coverage of the Digital Turkish Lira R&D Project into areas such as blockchain technology, the use of distributed ledgers in payment systems, and integration with instant payment systems. The Central Bank Digital Turkish Lira R&D Project would be accepted as an initial step to establishing a government-backed stablecoin in Türkiye.

Although there are no crypto assets that are backed by the government or a central bank, the crypto asset BiLira, which is a private initiative, was established as the first stablecoin backed by the Turkish Lira and is transferable on the blockchain.

Cryptocurrency regulation

As explained above, the Central Bank Regulation defines crypto assets as "*intangible assets that are created virtually using distributed ledger or similar technologies and are distributed over digital networks, and that are not qualified as money, registered money, electronic money, payment instrument, security or any other capital markets instrument*" and it is accepted that the Central Bank Regulation prohibits only direct or indirect use of crypto assets as payment instruments, excluding the purchase, sale, offering, transfer, or custody of crypto assets and the crypto asset exchange platforms providing such services.

Despite the definition of crypto assets provided in the Central Bank Regulation, the Istanbul Enforcement Law Court ruled that crypto assets are seizable by comparing their nature to securities with the following explanation: "*...such currencies are evaluated within the scope of commodities/securities and are considered as a type of digital currency or virtual money. In terms of Enforcement and Bankruptcy Law, crypto assets fulfill the criteria that having an economic value on its own in order for a property or right to be seized regardless of how it is defined in the economic field*."

Although the definition made by the Court contradicts the definition in the Central Bank Regulation, debates regarding the definition and nature of crypto assets both in academic and economic fields constitute the initial steps of legal recognition by the Republic of Türkiye. For instance, following the Central Bank Regulation, Presidential Decree "The Amendment to the Regulation on Measures Regarding Prevention of Laundering Proceeds of Crime and Financing of Terrorism" ("**Amendment to the Regulation on Measures**") was published in the Official Gazette dated May 1st, 2021 and entered into force on the same day. The Amendment to the Regulation on Measures imposes specific obligations on CASPs within the scope of Law No. 5549 on the Prevention of Laundering of the Proceeds of Crimes ("**Law No. 5549**"). However, no statutory definition of CASPs was found in the Amendment to the Regulation on Measures until the Financial Crimes Investigation Board ("**FCIB**") published the Guide on Main Principles Regarding the Prevention of Money Laundering and Financing of Terrorism for CASPs ("**AML Guide**"). According to definition under said Guide, CASPs "*intermediate the trading of crypto assets through electronic trading platforms*".

Sales regulation

There is currently no specific regulation dedicated to the sale of crypto assets or tokens, which are thus covered by the more general Turkish Code of Obligation No. 6098, the CML and commodity regulations (please see "Government attitude towards crypto assets" above). However, in its bulletin numbered 2018/42 on September 27th, 2018, the CMB provided that initial coin offerings/sales ("**ICOs**") are the sales of virtual (crypto) assets in exchange for fiat currency or other crypto assets in order to finance a project. While stating that ICOs are speculative, highly risky, and generally advertised with a "white paper", which relates to a prospectus, the CMB further evaluated that the structure of "white papers" differs in accordance with various utilities and applications of the crypto assets issued by ICOs, including, but not limited to, crypto assets that represent: a share in a company; a stake in a project; a right to access a service; and/or a tangible asset/product. Moreover, the regulatory treatment of any business models involving crypto assets and each offering must be assessed on a case-by-case basis, considering the diversity, complexity and rapid evolution of business models and the technical and economic design of the instruments offered.

Furthermore, in the abovementioned bulletin, asserting that ICOs that fall under the jurisdiction of the CMB might be associated with the crime of "*unauthorized capital markets activity*", the CMB provided that ICOs resemble public offerings and crowdfunding activities. However, although the Crowdfunding Communiqué (III-35/A.2), published in the Official Gazette dated October 27th, 2021 and numbered 31641, was recently introduced, its scope does not apply to ICOs. Therefore, there is currently no applicable law on the sale of crypto assets by means of an ICO.

It is worth mentioning that a debate regarding the legality of providing and/or selling different usages/products of crypto assets (derivates and staking) and crypto-backed services in Türkiye is currently being held between the participants of the ecosystem. Even though it is not crystal clear, there is a strong belief in the ecosystem that, since derivative instruments are defined as "*instruments the values of which depend on the price or return of a security, commodity or an underlying asset and/or depend on an index level which is formed by items or on changes in this index level*", the CMB may consider derivative transactions on crypto assets as a "derivative instrument" under Article 3.1(u) of the CML and classify them as a "security" under Article 3.1(ş) of the CML. In the event that the CMB acts in accordance with the aforementioned approach, CASPs providing customers with derivative products may be regarded as committing the crime of "*unauthorized capital markets activity*" and may be charged with "*imprisonment from two years up to five years and be punished with a judicial fine from five thousand days to ten thousand days*" in accordance with Article 109.2 of the CML.

Taxation

The third paragraph of Article 73 of the Turkish Constitution frames the principle of the legality of taxation by stating that taxes, fees, duties, and other such fiscal obligations shall be imposed, amended, or revoked by law. In Turkish tax law doctrine, it is also accepted that not only the main elements of the tax but also the duties and procedural issues, such as the assessment, notification, accrual, and collection of the tax, and sanctions arising from the taxation, should be regulated by law. In this regard, there is no tax regime regarding taxation of crypto assets in Türkiye as there are no specific tax regulations in force concerning crypto assets and the exchange of crypto assets.

In principle, the taxation of crypto assets depends on the nature of these assets and how they are acquired or exchanged. Therefore, the definition of crypto assets is significant for understanding how they fit within Türkiye's current tax regime. Considering the definition under the Unofficial Draft Legislation, it is hard to accept that crypto assets will be qualified as commodities since they are defined as "*an intangible asset representing a value or right that can be created and stored virtually through distributed ledger technology or any other similar technology and that can be distributed over digital networks*". Furthermore, the principle of the legality of taxation requires that no tax can be levied without that tax having been enacted by the legislative branch. In this regard, the uncertainty as to whether crypto assets meet taxation requirements should be clarified by law.

However, on September 23rd, 2020, the Edirne Tax Office published its official opinion ("**Official Opinion**") stating that "*Bitcoin assets should be declared with an inheritance and transfer tax return because the term commodities refer to all other rights and receivables that can be subject to movable and immovable property as per the Article 3.1 of the Inheritance and Transfer Tax Law No. 7338*". As it is understood from the Official Opinion, it can be deduced that the definition of commodity covers crypto assets pursuant to Article 3.1 of Inheritance and Transfer Tax Law No. 7338. However, from our perspective, reaching such conclusion without enacting the specific rules as to how crypto assets are treated for the purposes of taxation contradicts the legality principle of taxation and prevents us from accepting that crypto assets are qualified as commodities.

According to the Income Tax Law, all types of income, regardless of their nature, are subject to income tax. In this regard, all economic value generated from crypto assets may also be subject to income tax. However, there are no specific provisions in the Income Tax Law governing the taxation of income generated from crypto assets. Therefore, there is no legal regulation on the declaration of crypto asset holdings or funds and revenues generated therefrom for personal income taxation.

From a corporate tax point of view, the nature of crypto assets should be determined for the taxation of income generated from crypto assets. In the event that crypto assets are qualified as securities, they will be subject to the same taxation principles as securities. So, the income derived from the increase in the value of crypto assets will be taxed as commercial income. In the light of the opinions and practices of the tax authorities, taxpayers are able to utilise losses from crypto asset trading to offset such profits. Please note that tax is levied only when income is realised from the sale of crypto assets. Holding crypto assets will not create a tax liability until the realisation of income.

In the event that crypto assets are considered commodities, the continuity of the activity realised with crypto assets will change the nature of the gain, which will be taxed according to the Corporate Income Tax Law. If there is no continuity component in the commercial activity, the gain acquired by crypto assets will be accepted as incidental gain. On the other hand, the profit will be a commercial gain if the purchase and sale transactions are performed continuously to benefit from an increase in the value of crypto assets.

On the other hand, value-added tax ("**VAT**") is an indirect consumption tax that is levied on both the supply and the importation of goods and services listed in Article 1 of Value Added Tax Law No. 3065. Similar to the explanation on the corporate tax perspective above, VAT liability and the procedures and principles regarding VAT treatment will depend on how crypto assets are classified. In principle, from a Turkish taxation perspective, crypto asset transactions are not covered by VAT if they are exchanged for other virtual currencies or

fiat currencies, which will likely be deemed a money remittance transaction since it is not listed in Article 1 of Value Added Tax Law No. 3065. However, commission received by CASPs due to the provision of wallet services, which are defined as a software program that allows crypto asset users to store crypto assets, send and receive crypto transactions, and offer clearing services for crypto assets to third parties, is taxable within the scope of Value Added Tax Law No. 3065.

Finally, it should be taken into account that the establishment of a transparent taxation policy on crypto asset incomes and the influx of high transaction volumes from around the world to Türkiye, even if the taxation is based on the filing method, will strengthen the opportunities for both direct and indirect tax revenues to be brought to the Turkish Treasury, according to the "Digital Assets Report"[8] published by the Banks Association of Turkey ("**TBB**") on February 7th, 2022.

Money transmission laws and anti-money laundering requirements

Law No. 5549 and the Regulation on Measures Regarding Prevention of Laundering Proceeds of Crime and Financing of Terrorism ("**Regulation on Measures**"), published in the Official Gazette dated January 1st, 2008 and numbered 26751, provide the legal standards on AML/CTF. The competent authority to supervise the application of Law No. 5549 is FCIB, operating under Ministry of Treasury and Finance of the Republic of Türkiye. It is important to note that FCIB may initiate *ex officio* investigations regarding CASPs to monitor their compliance with AML/CTF requirements without receiving a complaint and may impose monetary sanctions on CASPs when it is detected that they fail to comply with such requirements. For instance, FCIB imposed total administrative fines of approximately €1,125 million on well-known CASPs within the scope of an *ex officio* audit due to their failure to fulfil its AML/CTF requirements on February 17th, 2022.

In order to prevent the risk of laundering the proceeds of crime and financing terrorism through crypto assets, Presidential Decree No. 3941 was published[9] in the Official Gazette dated May 1st, 2021 and numbered 31471 and amended Article 4 of the Regulation on Measures, which determines the term "obliged parties". With this amendment, the scope of application of the Regulation on Measures has been expanded to ensure that the obligations defined therein also apply to CASPs. Therefore, CASPs are considered "obliged parties" under the Regulation on Measures and shall be responsible for the prevention of laundering proceeds of crime and financing terrorism.

According to the Regulation on Measures, CASPs should also comply with the prevention measures and obligations stipulated under the said Regulation and shall be subject to investigation by FCIB. The current obligations foreseen for CASPs are as follows:

(i) conducting due diligence proceedings for their customers and identifying and verifying them (Know-Your-Customer ("**KYC**"));
(ii) assessing and reporting suspicious transactions to FCIB;
(iii) providing information and documents when requested;
(iv) retaining customer transaction documents, books and records for eight years and submitting them upon request; and
(v) reporting transactions that exceed the amount determined by the Ministry of Treasury and Finance of the Republic of Türkiye.

In order to implement these obligations, FCIB has published two guides detailing the obligations of CASPs.

FCIB's AML Guide for CASPs

To clarify, the obligations of CASPs provided under the Regulation on Measures, FCIB, the competent authority regarding measures for the prevention of money laundering and financing terrorism, published the AML Guide. Without any prejudice to the provisions of simplified measures for the KYC procedure (please see "Simplified KYC procedures for the customers of CASPs" below), the important requirements for CASPs regulated in the AML Guide are briefly provided below:

- The main obligations of CASPs are (1) customer identification (KYC), (2) reporting suspicious transactions, and (3) providing information and documents.
- KYC processes must be completed before entering into a contract (establishing a business relationship) or making a transaction. The accuracy of an individual's name, surname, date of birth, T.R. identification number (for Turkish citizens), and the type and number of identity documents must be verified with documentation.
- After originals or notarised copies of identity documents subjected to verification are submitted to CASPs, their photocopy or electronic image shall be received or information regarding the identity shall be recorded for submittal to the authorities when requested.
- The accuracy of an address declared in a permanent business relationship must be verified through (i) a certificate of residence, (ii) an invoice under the individual's name related to a subscription-based service such as electricity, water, natural gas, or telephone issued within three months of the transaction, or (iii) other documents and methods deemed appropriate by FCIB.

Reporting suspicious activity to FCIB is another important principle to prevent money laundering and terrorist financing. CASPs are also obliged to provide continuous information to FCIB, in addition to reporting suspicious transactions as described above. Therefore, in cases where the CASPs report a suspicious transaction while providing continuous information, they shall still be obliged to report such a suspicious transaction separately from the report that is continuously submitted to FCIB.

In cases where a suspicious transaction is encountered, CASPs must report the related information to FCIB by filling out the Suspicious Transaction Reporting Form as per the information and evidence it obtained to the extent possible.

It should also be emphasised that:

- the term "transaction" in "suspicious transaction" is not limited to a single transaction and can include more than one transaction; and
- a single Suspicious Transaction Reporting Form must be completed for transactions that raise suspicion when multiple transactions are considered together.

Submissions must be made by a legal representative of the related CASP, either physically or via an online system known as EMIS.ONLINE. The procedure for reporting a suspicious transaction is confidential and may not be disclosed to any party other than an FCIB inspector or the Court if the ongoing procedure is pending. The procedure to report suspicious transactions is further explained in FCIB's Suspicious Transactions Guide.

FCIB's Suspicious Transactions Guide for CASPs

The latest guideline, which entered into effect on April 18th, 2022, is titled the "Guide for Suspicious Transaction Reports of Crypto Asset Service Providers" ("**Suspicious Transactions Guide**"), in which FCIB sets out the principles and requirements to report suspicious transactions.

Aligning with the AML Guide, the Suspicious Transactions Guide also requires CASPs to report suspicious transactions to FCIB within 10 days at the latest, or immediately in the event of a non-delayable case. In cases where new information and findings concerning the reported transactions are obtained following the submission of the Suspicious Transaction Report, an additional Suspicious Transaction Report shall be filed and sent to FCIB without delay by addressing that the latter form is an additional report to the previous one. Furthermore, the Suspicious Transactions Guide provides more details on the procedure of submitting a customer's suspicious transaction to FCIB.

Accordingly, suspicious transactions must be reported by the legal representative of the obliged legal entity using the Suspicious Transaction Reporting Form, which includes the amounts concerned, the name/title of the transaction owner and the justification of the suspicion. In cases where FCIB authorises the relevant CASP, these Suspicious Transaction Reports can also be submitted via EMIS.ONLINE, FCIB's online operating system. Otherwise, they must be submitted via wet-signed papers or the registered email address. To gain authorisation and access to the EMIS.ONLINE system, the legal representatives of the obliged legal entity must prepare the Suspicious Transaction Reporting Commitment Form attached to the Suspicious Transactions Guide and submit it to FCIB with the documents specified in the form. Whether sent in paper form or electronically, a copy of the suspicious transaction notifications shall be preserved by CASPs for eight years.

In the event that CASPs believe that there are serious indications supporting the suspicion, the relevant CASP can send the Suspicious Transaction Report with a postponement request. However, the justifications should also be demonstrated.

Finally, considering that the FATF updated the interpretive note to "Recommendation 15" in its updated guidance for a risk-based approach in October 2021 and clarified the international standards on the "travel rule" of virtual (crypto) assets, one might expect the Republic of Türkiye, as a member of the FATF since September 24th, 1991, to adopt new regulations and guides in line with recent developments in the ecosystem. Keeping in mind that the "travel rule" of crypto assets in the EU provides a stricter approach to achieve higher standards on AML/CTF[10] by means of traceability, threshold limits and verification requirements of "un-hosted wallets" by CASPs, in order to achieve regulatory harmonisation between the European and the Turkish market, provisions mirroring the standards of the "travel rule" of either the EU or the FATF are expected to be implemented in Türkiye as well.

Simplified KYC procedures for the customers of CASPs

Pursuant to Article 26 of the Regulation on Measures, obliged parties, including CASPs, may be allowed to take simplified measures in terms of obligation on KYC principles under Law No. 5549. Simplified measures to be complied with by the obliged parties within the scope of KYC have been clarified by FCIB General Communiqué No:5 ("**Communiqué No. 5**") published in the Official Gazette dated April 9th, 2008 and numbered 26842. CASPs that are "*required to carry their activities exclusively in electronic environment*" may benefit from simplified measures regarding the KYC principle, in cases where they meet the following conditions of Article 2.2.10 of Communiqué No. 5:

- Executing an agreement with a bank located in Türkiye under which collection and payment transactions for goods and services are conducted in an electronic environment.
- Making all collections and payments through a bank account or credit card account that is compatible with the identity of the person whose membership has been accepted upon verified identity information.

- During the membership applications of the customer received in an electronic environment, verifying the natural person's (i) name and surname, (ii) nationality, (iii) date of birth, and (iv) T.R. identification number (foreign identification number for foreigners) through the identity sharing system database of the Ministry of Internal Affairs, General Directorate of Population and Citizenship Affairs ("**NVI**").

Pursuant to Article 2.2.10 of Communiqué No. 5, "*for the confirmation of the customer's identity information, obtaining a signature sample in accordance with the procedure set forth in Article 6 of the Regulation*" is not obligatory. Within this scope, in a simplified method for the KYC procedure, the documents listed above and stipulated in Article 6 of the Regulation on Measures shall be verified without the need for a signature sample. Therefore, CASPs who meet the conditions mentioned in Communiqué No. 5 shall benefit from the simplified method while fulfilling the KYC and identification obligations provided by Law No. 5549, and obtaining the signature sample of the customer and the documents envisaged in the Regulation on Measures, such as identity card, driver's licence, and passport, shall not be necessary for the verification procedure if the information is verified through the NVI database. However, most CASPs operating in the Turkish market still collect the documents stipulated in Law No. 5549 from their customers to fulfil the KYC identification procedure without taking full advantage of the simplified measures.

On the other hand, some CASPs continue to collect the documents listed in the Regulation on Measures for fulfilling the identification obligations as a precautionary application while they apply the simplified measures for the KYC procedure. Since the documents collected contain personal data of the customers, obtaining such documents may raise liability issues for CASPs under Personal Data Protection Law No. 6698. We believe that such CASPs might be under an obligation to acquire the explicit consent of the customers rather than utilising the "*collection of personal data based on the legal reason*" as fulfilment of legal obligations or legitimate interests stipulated by law. Because their personal data processing activities would be challenged by the data minimisation principle, this means that personal data shall be adequate and limited to what is necessary in relation to the purposes for which they are processed.

It is important to point out that Article 2.2.10 of Communiqué No. 5 does not govern the identification procedure for non-residents. Therefore, one might state that the simplified KYC procedure should not be applicable if the customer concerned is a foreign and non-resident person.

Lastly, on November 23rd, 2022, FCIB issued an announcement on FTX Türkiye and had sought approval from the Istanbul Chief Public Prosecutor's Office to initiate "an investigation for various antecedent crimes and laundering the property values arising from the crime" and to "confiscate the suspicious assets" in accordance with Law No. 5549.

Promotion and testing

Currently, there is no "sandbox" or other incentive to promote research and investment in crypto assets. However, considering that the legal background of the Istanbul Financial Center is now governed by Istanbul Financial Center Law No. 7412, which entered into force on June 22nd, 2022, the Republic of Türkiye subsequently established the Istanbul Financial Center in the second quarter of 2023, creating an innovative hub for future fintech development. Most importantly, in its 2021 Annual Report on the Fintech Ecosystem of Türkiye, the Finance Office of the Presidency of the Republic of Türkiye provides that a regulatory sandbox, aiming to improve fintech products, services and business models to

revitalise the sector and identify and transform improvement areas in regulations, would be located in the Istanbul Financial Center. The Finance Office of the Presidency of the Republic of Türkiye expresses that, with this structure, it would be easier to develop innovative financial products, trigger competition and innovation, and develop policies based on output.

Ownership and licensing requirements

Currently, there is no specific provision in capital market regulations regarding investment managers owning crypto assets for investment purposes. However, collective investment funds, including alternative investment funds, are prohibited from investing in crypto assets or crypto asset-backed products, and exchange traded funds that have crypto assets in their portfolio and shares of CASPs, according to the CMB Decree dated November 27th, 2021.

Furthermore, according to the Unofficial Draft Legislation, which was first brought to public attention in December 2021 without any official press release, the CMB will have the authority to determine the procedures and principles regarding investment advisory and portfolio management for crypto assets.

Once the Unofficial Draft Legislation comes into force, individuals and institutions (including, but not limited to, investment managers, investment advisors or fund managers, and CASPs) that operate in the crypto asset industry without obtaining a licence or permission from the CMB will face penalties and administrative measures, since they will be subject to the supervision of the CMB in terms of compliance with the CML.

Mining

Currently, the mining of crypto assets is not regulated. Mining in itself does not fall under the definition under the CML.

Since ecological threats are escalating day by day, various blockchain projects are being established in a proof-of-stake ("**PoS**") consensus rather than a proof-of-work ("**PoW**") consensus or migrating to a PoS consensus (such as ETH 2.0). Therefore, a different assessment may be conducted on blockchains with a PoS consensus.

Regarding staking on blockchains with a PoS consensus, even though the rewards generated with staking activities may be regarded as an "interest" of a "deposit account" and claimed as an activity of "accepting deposits" under Article 4.1/(a) of Banking Law No. 5411 ("**Banking Law**"), Article 3.1 of the Banking Law defines "deposit" as "***money*** *accepted by announcing to the public, verbally or in writing or in any manner, in return for or without a consideration or to be returned on a certain date of maturity or whenever it is called*". Therefore, considering that crypto assets are not treated as money in accordance with the Central Bank Regulation, the rewards generated by staking crypto assets should not be regarded as banking activity.

Additionally, there should be a different approach between on-chain staking and custodial staking activities. At this point, it should be emphasised that on-chain staking activities are performed on a (so-called) decentralised network with a PoS consensus directly by the users (validators) without providing their private keys to a third party. Therefore, in our opinion, differentiation between on-chain staking and custodial staking activities is a must, the latter being a customer activity, by providing their crypto asset private keys in exchange for an "interest" rate determined by the relevant CASP rather than the rewards being the natural product of participation in a PoS consensus mechanism.

However, it should be stated that there is not yet a clear approach that differentiates between on-chain staking (staking on blockchain) and custodial staking (staking with products provided by CASPs). In this vein, it is not crystal clear whether custodial staking activities will be subject to the CML, the Banking Law or another legislation.

Border restrictions and declaration

There are currently no border restrictions or obligations to declare crypto asset holdings under Turkish law.

Reporting requirements

The AML Guide (please see "Money transmission laws and anti-money laundering requirements" above) provides that, since CASPs and their customers enter into agreements and customer transactions are carried out based on these agreements, business relationships between CASPs and their customers are regarded as "continuous business relationships". In this regard, CASPs are also obliged to provide continuous information to FCIB considering the relation between CASPs and their customers, accepted as "continuous business relationships".

Therefore, a CASP must submit a report by filing to FCIB if a suspicious transaction is detected under the AML/CTF regulations discussed above (please see "FCIB's Suspicious Transactions Guide for CASPs" above) while providing continuous information. Other than reporting suspicious transactions, there is no specific provision regarding the reporting requirement for crypto asset payments for either CASPs or parties to the transaction.

Estate planning and testamentary succession

There is no established law with respect to the treatment of crypto assets under Turkish inheritance law. Given the fact that there is no consensus on the definition of crypto assets from a legislative perspective, there is ambiguity when determining whether crypto assets will be a part of the deceased's estate. Considering the anonymous nature of crypto assets, the identification and collection of crypto assets as inherited property would be a material issue, unless the relevant private key or password is known to the deceased, even though it is accepted that crypto assets will be succeeded to by the deceased.

On the other hand, on September 23rd, 2020, the Edirne Tax Office accepted under the Official Opinion that: "*Bitcoin assets should be declared with an inheritance and inheritance tax will be imposed upon the estate of a deceased person in respect of Bitcoin that were held by such person*." According to the mentioned Official Opinion, "Bitcoin" can be accepted as a commodity because, as per Article 3.1 of the Inheritance and Transfer Tax Law, the term "commodity" refers to all other rights and receivables that can be subject to movable and immovable property. As explained under the "Taxation" section above, reaching such a conclusion without enacting the specific rules as to how crypto assets are treated for the purposes of taxation shall contradict the legality principle of taxation and prevents to accept that crypto assets are qualified as commodities.

Moreover, the Central Bank Regulation and the Unofficial Draft Legislation define crypto assets mainly as "intangible assets". In this regard, theoretically, crypto assets can be included in the heritage similar to other assets of the deceased person and can be subjected to estate planning and testamentary succession. However, the legal framework and the statutory definition must be implemented so that issues related to inheritance law can be properly explained.

Lastly, it is important to mention that, on November 13th, 2020, the term "digital asset" was defined for the first time by the 6th Civil Chamber of the Antalya Regional Court of Justice[11] as "*other assets that are solely available in digital form and stored electronically, such as videos, photos, emails, personal social media accounts*" and the Court ruled that a number of digital assets were part of the deceased's estate as digital inheritance, "*passing down of the digital assets to inheritors; being subject to inheritance*". In the event that crypto assets are qualified as "digital assets", it would be possible to open the door for crypto assets to be included in succession and inheritance.

* * *

Endnotes

1. Please see "Crypto usage in Turkey increased elevenfold in a year, new survey shows", https://cointelegraph.com/news/crypto-usage-in-turkey-jumped-by-elevenfold-in-a-year-new-survey-shows (last accessed on July 25th, 2023); and "Turks flock to cryptocurrencies in search of stability", https://www.ft.com/content/02194361-a5b9-4bf0-9147-f36ba7759cf1 (last accessed on July 25th, 2023).
2. Please see "Tales from the crypto: lira crisis fuels Bitcoin boom in Turkey", https://www.theguardian.com/business/2022/jan/21/tales-from-the-crypto-lira-crisis-fuels-bitcoin-boom-in-turkey (last accessed on July 25th, 2023).
3. Please see "Turkey pushes for bigger say over crypto market with draft bills", https://www.bloomberg.com/news/articles/2022-05-25/turkey-pushes-for-bigger-say-over-crypto-market-with-draft-bills#xj4y7vzkg (last accessed on July 25th, 2023).
4. Please see BRSA Public Announcement dated November 25th, 2022, https://www.bddk.org.tr/Duyuru/EkGetir/510?ekId=530 (last accessed on July 25th, 2023).
5. Please see Press Release on Central Bank Digital Turkish Lira R&D Project, https://www.tcmb.gov.tr/wps/wcm/connect/EN/TCMB+EN/Main+Menu/Announcements/Press+Releases/2021/ANO2021-40 (last accessed on July 25th, 2023).
6. ASELSAN is a company of the Turkish Armed Forces Foundation, established in 1975 in order to meet the communication needs of the Turkish Armed Forces by national means.
7. HAVELSAN is affiliated to the Turkish Armed Forces Foundation, established in 1982 to develop and produce technology in the defence, security and information sectors, along with high technology and software solutions developed in-house.
8. Please see "*Dijital Varlıklara Yönelik Bankacılık Açısından Genel Bakış, Potansiyel İş Modelleri ve Dijital Varlıkların Hukuki Açıdan Değerlendirmesi*", https://www.tbb.org.tr/Content/Upload/tos/Dijital%20Varl%C4%B1klar%20Raporu.pdf (last accessed on July 25th, 2023).
9. Please see "Türkiye adds crypto firms to money laundering, terror financing rules", https://www.reuters.com/technology/Türkiye-adds-crypto-firms-money-laundering-terror-financing-rules-2021-05-01/ (last accessed on July 25th, 2023).
10. Please see "Crypto assets: deal on new rules to stop illicit flows in the EU", https://www.europarl.europa.eu/news/en/press-room/20220627IPR33919/crypto-assets-deal-on-new-rules-to-stop-illicit-flows-in-the-eu (last accessed on July 25th, 2023).
11. The 6th Civil Chamber of the Antalya Regional Court of Justice, File No. 2020/1149, Decision No. 2020/905, dated November 13th, 2020.

Alper Onar
Tel: +90 532 463 80 74 / Email: aonar@aksan.av.tr

Alper joined Aksan Law Firm in March 2021. Before joining Aksan, he worked for five years as a Director responsible for the Finance Law Team at PwC, for nine years as Senior Legal Counsel at the Capital Markets Board of Türkiye, and two years as an Attorney at Law in a local law firm.

Alper specialises in securities, investments, mergers and acquisitions, derivatives and structured finance transactions. He is experienced in public offerings, private equity and restructuring, and anti-money laundering. Alper currently advises listed companies and financial institutions, including banks, investment firms, venture capital funds, asset management companies, payment and e-money institutions, and crypto asset exchanges, in the areas of corporate and financial law, blockchain and crypto assets. He has been a member of the TÜBİTAK 1514 GİSDEG Program Group Executive Board for the past three years and is currently a member of the TÜSİAD Capital Markets Working Group.

Emre Subaşı
Tel: +90 506 245 19 21 / Email: esubasi@aksan.av.tr

Emre worked at the CMB for five years before resigning to become part of the founding team of Turkish Mercantile Exchange (TMEX), where he served as Chief Legal Counsel for about three years.

At CMB, he carried out extensive studies on the public offerings, audit and surveillance of public companies and also worked on capital market instrument issuances, capital market crimes, and judicial and administrative litigation processes.

At TMEX, he prepared all the internal legislation, updated related regulations, and managed to establish business processes with market participants. Likewise, he prepared all the legal processes of TMEX and participated in negotiation processes in all of TMEX's agreements, mostly regarding software projects and business development activities.

Currently, Emre mainly provides services in the fields of start-up investments, crypto asset platforms, acquisitions, capital market law, and corporate law.

Aksan Law Firm

Levent, Konaklar Mahallesi Zeki Müren Sokağı No:7 Aksan Binası 4, Levent, 34330 Beşiktaş/İstanbul, Türkiye
Tel: +90 212 249 83 83 / URL: www.aksan.av.tr

United Kingdom

Charles Kerrigan, Christina Fraziero,
Olivia Hamilton-Russell & Antonia Bain
CMS LLP

Government attitude and definition

Government attitude

The regulation of cryptoassets in the UK has developed alongside the evolution of the technology itself. Overall, UK regulators have attempted to balance supporting innovation with protecting consumers and maintaining financial stability. In 2018, the Cryptoassets Taskforce (the **Taskforce**) brought together HM Treasury (**HMT**), the Financial Conduct Authority (the **FCA**), and the Bank of England (the **BoE**) to coordinate the UK's approach to regulating cryptoassets and distributed ledger technology (**DLT**) as it relates to financial services. In April 2022, the UK government expressed its intention to make the UK a global hub for cryptoasset technology and investment and in February 2023, HMT released a consultation paper and call for evidence on a future financial services regulatory regime for cryptoassets (the **Consultation**), which seeks to deliver on the aforementioned ambitions. UK policymakers and regulators have identified the opportunity presented by cryptoasset technology and intend to encourage growth, innovation, and competition in the industry, while (i) protecting UK consumers by clearly presenting the risks involved to ensure that they make well-informed decisions, and (ii) maintaining stability and market integrity.

Definition

At the time of writing, there is no accepted global definition of a "cryptoasset";[1] however, there is increasing consensus on the basic elements of the definition in UK and international legislation. The Financial Services and Markets Bill (the **FSMB**), which received Royal Assent on 29 June 2023, defines cryptoassets as:

> "*[A]ny cryptographically secured digital representation of value or contractual rights that –*
>
> *(a) can be transferred, stored or traded electronically, and*
>
> *(b) uses technology supporting the recording or storage of data (which may include distributed ledger technology).*"

This definition is similar to the definition of cryptoasset used in the Money Laundering, Terrorist Financing and Transfer of Funds (Information on the Payer) Regulations 2017 (as expanded by the Money Laundering and Terrorist Financing (Amendment) Regulations 2019 to cover cryptoassets) (**MLRs**), the principal difference being that the FSMB definition references a wider range of underlying technology.

The Consulation identifies four broad types of "cryptoassets":

- Security tokens, which amount to a "specified investment" as set out in the Financial Services and Markets Act (2000) (Regulated Activities) Order (the **RAO**). These may provide rights such as ownership, repayment of a specific sum of money, or entitlement

to a share in future profits. They may also be transferable securities or financial instruments under the EU's Markets in Financial Instruments Directive II (**MiFID II**).

- Exchange tokens, often referred to as "cryptocurrencies" such as Bitcoin, Litecoin, or others, which use a technology such as DLT to support the recording or storage of data and are not issued or backed by a central bank or other central body. They are used as a means of exchange or for investment purposes but do not provide the types of rights or access provided by security tokens or utility tokens. Exchange tokens include stablecoins and algorithmic and asset-referenced tokens.
- Utility tokens, which provide digital access to a specific service or application (*e.g.*, digital advertising or file storage) and use a technology such as DLT to support the recording or storage of data. They do not provide the rights or features associated with a security token (*e.g.*, share or ownership rights) and do not function as a means of payment, although they can be traded on cryptoasset trading venues for investment purposes. Utility tokens include governance tokens and fan tokens.
- Non-fungible tokens (**NFTs**), which confer digital ownership rights of a unique asset (*e.g.*, a piece of digital art) using a technology such as DLT to support the recording or storage of data. NFTs do not provide the rights or features associated with a security token and do not function as a means of payment.

Certain types of cryptoasset identified above may also fall within the definition of e-money under the E-Money Regulations 2011 (the **EMRs**). The FCA's Perimeter Guidance for Cryptoassets (PS 19/22) (the **Guidance**) sets out more detail on the different types of cryptoassets and their interactions with the existing regulatory perimeter.

Central bank digital currency

In addition to its role as a consultee and member of the Taskforce, the BoE is considering the introduction of a central bank digital currency (**CBDC**), although this has not yet been implemented.

Cryptocurrency regulation

The UK does not currently regulate crypto *per se*; rather, cryptoassets and related activities may fall within existing regimes where their specific characteristics dictate so. Currently, cryptoasset activities performed in the UK are regulated under two distinct regulatory frameworks:

- The first framework applies to all cryptoassets and is determined by what is done with the cryptoasset and whether that creates a money laundering risk. Firms that fall within this regime are required to register with the FCA under the MLRs.
- The second framework applies depending on the characteristics of a cryptoasset, and whether it falls within the definition of a "specified investment" under the RAO.

In addition to the RAO and MLRs, the advertisement of certain products or activities, where they are aimed at or are otherwise "capable of having an effect in the UK", may be subject to certain restrictions set out in the Financial Services and Markets Act 2000 (Financial Promotion) Order 2005 (the **FPO**). This will depend on whether the product or activity falls within the definition of "controlled investment" or "controlled activity" in section 21 of the Financial Services and Markets Act 2000 (**FSMA**) (which prohibits unauthorised financial promotions).

The UK's proposed approach to cryptoasset regulation is detailed in the Consultation. One of the core design principles of the new regulatory regime is "same risk, same regulatory outcome", meaning a focus on achieving the same regulatory outcome where possible, regardless of the technology used.

In contrast with the EU's approach of introducing a bespoke regulatory framework for cryptoassets (**MiCAR**), the UK government intends to adopt a phased approach and bring cryptoassets within the existing regulatory framework established by FSMA and the RAO, as follows:

- First, the government has introduced legislation[2] to bring "qualifying cryptoassets" into the scope of the existing financial promotions regime under the FPO.
- Second, the government has legislated through the FSMB to introduce a regime that will allow for the regulation of fiat-backed stablecoins that are used for payments.
- Third, the government intends to introduce a regime to regulate broader cryptoasset activities, such as the trading of and investment in cryptoassets, which will focus on targeting activity areas associated with a higher degree of risk from both a consumer and market perspective. The proposed scope of cryptoasset activities to be regulated is broad and includes: (i) issuance activities; (ii) payment activities; (iii) exchange activities; (iv) investment and risk management activities; (v) lending, borrowing and leverage activities; (vi) safeguarding and/or administration (custody) activities; and (vii) validation and governance activities.
- Fourth, in more nascent areas of the market, the government will actively seek views to inform future policy development and will continue to strategically assess developments in the market to determine future phases of work, taking into consideration the views of industry, consumers, and regulators.

Sales regulation

The sale of cryptocurrency in the UK is subject to sales regulations that fall into three broad categories: (i) the financial promotions regime; (ii) prospectus regulation; and (iii) consumer protection and online/distance selling legislation.

Financial promotions

A financial promotion is an invitation or inducement that is communicated in the course of business to engage in investment activity. The financial promotion regime applies to communications with reference to certain activities involving "controlled investments" (such as shares, bonds or derivatives) and "controlled activities", both of which are set out in an exhaustive list in the FPO. Financial promotions capable of having an effect in the UK must:

- be issued by an FCA/Prudential Regulation Authority (**PRA**)-authorised person;
- be approved by an FCA/PRA-authorised person; or
- fall within an exemption from the financial promotion regime.

To determine whether the financial promotion regime applies to cryptoassets, it is necessary to determine whether the activities involve a "controlled activity" or "controlled investment" by referring to the FPO. Where a cryptoasset is a regulated "specified investment" (*i.e.*, a security token), then it will likely fall within the definition of "controlled investment" and, therefore, the remit of section 21 of FSMA.

On 7 June 2023, the government passed the Financial Services and Markets Act 2000 (Financial Promotion) (Amendment) Order 2023 (the **FP Amendment Order**), which will bring "qualifying cryptoassets" within the scope of the FPO with effect from 8 October 2023. Broadly, a "qualifying cryptoasset" is any cryptographically secured digital representation of value or contractual rights that is transferable and fungible, but does not include NFTs, cryptoassets that meet the definition of e-money, or an existing "controlled investment" (*i.e.*, a security token). This broad definition covers most cryptocurrencies not captured by the scope of the regime; therefore, financial promotions communications that are invitations

or inducements to engage in such activities will no longer be permitted unless they are issued by an FCA/PRA-authorised person, are approved by an FCA/PRA person, or fall within an exemption from the financial promotion regime. However, the FP Amendment Order carves out a bespoke exemption insofar as firms registered with the FCA under the MLRs may leverage their authorisation to approve and communicate their own promotions.

Breaching this restriction is a criminal offence punishable by a fine and/or up to two years' imprisonment. Additionally, breach of the prohibition may affect any officer, manager, or beneficial owners' ability to satisfy the "fit and proper requirements" laid out under the MLRs. Both HMT and the FCA have committed to adopt a hardline approach in enforcing the legislation when it takes effect.

Immediately following the passing of the FP Amendment Order, on 8 June 2023, the FCA published Policy Statement PS23/6 on "Financial promotion rules for cryptoassets" (the **Cryptoasset FP Policy Statement**), setting out its final policy position near-final Handbook rules.[3] The Cryptoasset FP Policy Statement confirms that the FCA intends to proceed as consulted with categorising cryptoassets as "Restricted Mass Market Investments" (**RMMIs**) and apply associated restrictions on their marketing to UK consumers, as set out in the FCA's Policy Statement PS 22/10 on "Strengthening our financial promotion rules for high-risk investments and firms approving financial Promotions".[4] Among other things, for first-time investors in RMMIs, and therefore cryptoassets, a personalised risk-warning pop-up and a 24-hour cooling-off period will be required. There will also be a ban on inducements to invest in these (*e.g.*, "refer a friend" bonuses).

Prospectus Regulation

FSMA and the onshored UK Prospectus Regulation require firms to make available an approved prospectus to the public, before (i) transferable securities are offered to the public, or (ii) a request is made for transferable securities to be admitted to a regulated market situated or operating in the UK.

These requirements relate to transferable securities and so, to determine whether this regime is applicable to cryptoassets, it must be established whether the relevant cryptoasset is a transferable security. If it is a transferable security and is offered to the public or admitted to trading on a regulated market, the issuer must publish a prospectus. Transferable securities are those captured in the definition set forth in the UK Markets in Financial Instruments Regulation (**MiFIR**). It is a criminal offence to make an offer or request admission to trading of transferable securities without an approved prospectus, although a number of exemptions are available (*e.g.*, public offers made to "qualified investors" or fewer than 150 persons). The Guidance sets out that only security tokens may be transferable securities.

In the Consultation, the government proposes to establish an issuance and disclosures regime for cryptoassets tailored to their specific attributes. As with traditional securities offerings, restrictions will be placed on public offerings of a cryptoasset and its admission to a cryptoasset trading venue without a prospectus. The proposed Designated Activities Regime (**DAR**) introduced by the FSMB and designed to enable HMT to designate certain activities in order to make regulations relating to the performance of that activity will be used as a basis to develop rules governing prospectus requirements as the existing onshored UK Prospectus Regulation will be replaced under the FSMB. Certain exemptions are intended to be available according to the type or scope of public offer, including offers below a *de minimis* monetary threshold, offers made only to "qualified investors", and offers made to fewer than 150 persons. Where there is no issuer (*e.g.*, Bitcoin), the trading venue would be required to take on the responsibilities of the issuer if they wish to admit the asset for trading.[5]

General advertising, online/distance selling and consumer protection legislation

Those marketing cryptoassets are also required to comply with the CAP Code and the Advertising Standards Authority (the **ASA**) guidelines.

The ASA provides various standards as to how cryptoassets may be promoted and advertised. Among other things, these standards provide that advertisement should not be misleading or contain false information and should not imply that crypto investments are riskless, or low-risk, trivial decisions. Any advertisement must also prominently and clearly state that:

- cryptocurrencies are unregulated in the UK;
- any profits may be subject to capital gains tax (**CGT**); and
- the value of investments is variable.

Outside the requirements of the UK financial regulatory framework, other legislation may be relevant to the sale or offering of cryptocurrency and services related to them:

- The Consumer Rights Act 2015 and the Consumer Protection from Unfair Trading Regulations 2008 apply in relation to consumers (individuals acting outside of their trade, business, craft or profession) and provide them with statutory rights and remedies against suppliers of goods, services and digital content. Further restrictions are imposed on the kinds of contractual terms that can be enforced against consumers.
- The Electronic Commerce (the **EC Directive**) Regulations 2022 apply more generally and impose requirements on businesses that offer or provide goods or services digitally. Whether the legislation applies depends on whether the business being conducted is subject to UK regulation.

Taxation

At the time of writing, there is no specific tax regime to govern how cryptoasset transactions are taxed; therefore, the current tax rules must be considered and applied (although some uncertainty remains as to their application). The UK tax authority, HM Revenue and Customs (**HMRC**), uses the same definition of cryptoassets adopted by the Taskforce, identifying four types of cryptoassets, namely exchange tokens, utility tokens, security tokens, and stablecoins. The classification of cryptoassets is not necessarily determinative of their tax treatment, which will depend on the nature and use of the cryptoasset in question.

HMRC has published some guidance relating to the taxation of cryptoassets, focusing on the taxation of exchange tokens. It is important to note that HMRC is not bound by its published guidance; however, it is useful for interpreting how HMRC might approach a tax case that will be decided on its facts.

HMRC does not treat exchange tokens as money or fiat currency; therefore, tax rules that apply to fiat currency do not apply to exchange tokens. Additionally, exchange tokens contributed to pension funds would not be treated as a tax-relievable contribution.

In April 2022, the government announced that it will explore ways to enhance the competitiveness of the UK tax system to encourage development of the cryptoasset market.[6] This includes:

- a review of how decentralised finance (**DeFi**) loans (where holders of cryptoassets lend the assets out for a return) are treated for tax purposes;
- a consultation on extending the scope of the Investment Manager Exemption (the **IME**) to include cryptoassets; and
- negotiation on a new OECD Crypto-Asset Reporting Framework (**CARF**), which is intended to amend the Common Reporting Standard (**CRS**) to ensure enhanced tax transparency and enable a level playing field in tax reporting globally.

DeFi

The transfer of cryptoassets for the purposes of lending or staking triggers a capital disposal and potentially a "dry tax charge" under CGT rules. Moreover, returns from lending or staking cryptoassets are not treated as interest as HMRC does not consider cryptoassets to be money or fiat currency. How the return is taxed will depend on whether the receipt has the nature of capital or revenue.

Responses from HMRC's first round of consultation in 2022 for reform favoured new legislation to create separate rules for DeFi lending and staking similar to those rules applicable to repos and stock lending. HMRC's second round of consultation closed in June 2023.[7]

IME

The IME is a statutory concession, which provides that a UK-based investment manager will not be treated as a UK representative of a non-UK resident fund if certain conditions are met. These conditions include limits as to the types of transaction that can qualify for the IME. A list of qualifying transactions is set out in the investment transactions list (the **ITL**). HMRC published regulations to implement this change in December 2022, which came into force on 1 January 2023.[8] Changes to the ITL for the purposes of the regulations will only apply to the IME and not to other tax whitelists. Notably, the regulations have adopted the wide definition of "cryptoasset" in CARF, save certain exclusions.[9]

CARF

In June 2023, the OECD published a revised version of CARF.[10] Broadly, CARF contains a suite of due diligence and reporting requirements that applies to entities and individuals dealing with cryptoassets. CARF also contains a Multilateral Competent Authority Agreement on automatic exchange of information (the **MCAA**) to facilitate the exchange of information between signatories to the MCAA. At the time of writing, the UK has yet to announce a timeline for implementing CARF into domestic legislation.

Taxation of individuals

HMRC guidance contains the following general points relating to how individuals who hold exchange tokens are to be taxed:[11]

- buying and selling cryptocurrency would most likely amount to personal investment activity (as opposed to trading activity) such that CGT would be payable on any gains an individual realises on disposal;
- if an individual is involved in a "trade" of exchange tokens, any trading profits would be subject to income tax, rather than CGT; and
- exchange tokens received as a form of payment from an employer would be subject to income tax and National Insurance contributions.

Disposals include (but are not limited to):

- selling exchange tokens for money;
- exchanging one type of cryptoasset for a different type of cryptoasset;
- giving tokens away to another person; and
- using exchange tokens to pay for goods or services.

A UK tax-resident but non-domiciled individual who claims the remittance basis of taxation is normally only subject to UK income tax and CGT in respect of non-UK-sourced income and capital gains (arising from the disposal of non-UK-situated assets), respectively, that have been remitted to the UK. HMRC guidance treats the situs of exchange tokens as being the jurisdiction in which the individual beneficial owner of the exchange tokens is tax-resident. Therefore, UK tax residents, regardless of their domicile status, would be

subject to UK income tax or CGT in respect of any non-UK-sourced income and capital gains (arising from the disposal of non-UK-situated cryptoassets), respectively, regardless of whether such income or gains have been remitted to the UK.

Individual taxpayers should keep detailed records in respect of every cryptoasset transaction.

Taxation of businesses

In respect of how transactions involving exchange tokens undertaken by companies and other businesses (including sole traders and partnerships) would be treated, HMRC has indicated the following:[12]

- corporation tax (**CT**) legislation, which relates to money or fiat currency, would not apply to cryptoassets as HMRC does not consider exchange tokens to be money;
- where activity such as buying and selling exchange tokens amounts to a "trade", the receipts and expenses of the trade will form part of the calculation of the trading profit in respect of that business for CT purposes;
- where the activity does not amount to a "trade", and is not charged to CT in another way, the activity might be treated as the disposal of a capital asset such that any gain arising from the disposal would be charged to CT as a chargeable gain;
- value-added tax (**VAT**) is due in the normal way on the supply of goods or services sold in exchange for cryptoassets;
- stamp duty and stamp duty reserve tax is unlikely to be chargeable on the transfer of exchange tokens. However, every case will be considered on its own facts and circumstances; and
- stamp duty land tax is not payable on transfers of exchange tokens as such transfers are not considered by HMRC to be land transactions; however, if exchange tokens are given as consideration for a land transaction, the tokens would fall within the definition of "money or money's worth" and would be chargeable to stamp duty land tax.

Money transmission laws and anti-money laundering requirements

AML requirements

The MLRs impose a general duty on cryptoasset businesses to maintain appropriate risk-based policies and procedures to prevent situations where their systems might be used for money laundering or terrorist financing. The MLRs transposed the provisions of the Fourth Money Laundering Directive ((EU) 2015/849) (**MLD4**) into UK law; their scope was further widened in January 2020 when the Fifth Money Laundering Directive ((EU) 2018/843) (**MLD5**) was incorporated into UK law. This brought businesses carrying on cryptoasset activity in the UK into scope of the MLRs, and a requirement to be registered with the FCA.

In-scope cryptoasset businesses are expected to have been complying with the MLRs since 10 January 2020. The MLRs define a cryptoasset as "*a cryptographically secured digital representation of value or contractual rights that uses a form of DLT and can be transferred, stored or traded electronically*".

The MLRs apply to businesses identified as being most vulnerable to the risk of being used for money laundering and terrorist financing purposes. In-scope businesses are referred to as "relevant persons", as listed in regulation 8(2) and (3). The implementation of MLD5 brought CEPs and CWPs (defined below) within scope of the MLRs as relevant persons; consequently, any person carrying out cryptoasset business that is captured in the definitions below are impacted.

A cryptoasset exchange provider (**CEP**) is a firm or sole practitioner who, by way of business, provides one or more of the following services, including where the firm or sole practitioner does so as creator or issuer of any of the cryptoassets involved:

- exchanging, or arranging or making arrangements with a view to the exchange of, cryptoassets for money or money for cryptoassets;
- exchanging, or arranging or making arrangements with a view to the exchange of, one cryptoasset for another; or
- operating a machine that uses automated processes to exchange cryptoassets for money or money for cryptoassets.

The FCA makes clear that businesses operating cryptoasset automated teller machines and peer-to-peer providers are in scope of the MLRs, as well as businesses that issue new cryptoassets such as initial coin offerings (**ICOs**) or initial exchange offerings (**IEOs**).

A custodian wallet provider (**CWP**) is a firm or sole practitioner who, by way of business, provides services to safeguard, or to safeguard and administer, either of the following when providing these services:

- cryptoassets on behalf of its customers; or
- private cryptographic keys on behalf of its customers to hold, store and transfer cryptoassets.

The FCA has stated that it will consider the commercial element, commercial benefit, the relevance to other business by the relevant firm, and the regularity/frequency of activities as factors impacting its decisions on whether cryptoasset activity is carried on.

Notably, a person might be a CEP or CWP, irrespective of whether they are otherwise regulated in the UK, if they carry on cryptoasset business that is in scope of the new definitions. Therefore, MLR requirements for cryptoasset businesses apply to both regulated and unregulated cryptoasset businesses in the UK.

To adhere to the MLRs, businesses must comply with various obligations, such as: making a registration; ongoing risk assessments; maintenance of appropriate policies; controls and procedures; staff training; customer due diligence; record keeping; and reporting. For example, on 30 August 2022, the Office of Financial Sanctions Implementation (**OFSI**) updated its guidance for financial sanctions under the Sanctions and Anti-Money Laundering Act 2018 (**SAMLA**) to reflect reporting obligation measures coming into force. The regulations extend the definition of "relevant firms" that have financial sanctions reporting obligations to include CEPs and CWPs, and they are therefore required to notify OFSI of certain information.

The Joint Money Laundering Steering Group published guidance that further clarified how the MLRs relate to cryptoassets. The guidance highlights the AML risks relevant in the sector and considers how CEPs and CWPs should interpret the AML requirements in an appropriate manner relating to cryptoassets.

Money transmission laws

Firms that engage in the transfer of money "by way of business", including money transmitters and money service businesses that are not subject to an exemption from registration, are supervised by the FCA under the PSRs and the EMRs.[13] These regulations aim to ensure the security and efficiency of payment services and e-money issuance within the UK. Money transmission businesses are subject to regular audits and compliance checks by the FCA to ensure they meet their regulatory requirements with respect to money laundering supervision (including customer due diligence, record keeping, and reporting suspicious activity).[14]

The FCA may determine that certain types of cryptoassets trigger the regulatory perimeter under the EMRs where they constitute e-money tokens (*e.g.*, fiat-backed stablecoins that are used for payments) and the PSRs where facilitating regulated payment services (*e.g.*, the provision of wallet services for stablecoins).[15] This determination by the FCA would depend on the specific characteristics of the cryptoassets and their use cases.

Promotion and testing

In line with the legislative intention, there are a number of initiatives that strive to encourage innovation in this area. Most of these initiatives are supported by the FCA, which established an Innovation Division in November 2018.

The FCA's Innovation Hub aims to provide direct support to innovative firms that are trying to launch into the market. It does so through several initiatives:

- The **Regulatory Sandbox** provides an opportunity for businesses of all sizes, authorised and unauthorised, incumbent or new players, to pilot the commercial and regulatory viability of their products and services in a live environment under supervision. To be accepted, the test project must have a clear objective and must confer a clear positive impact on consumers. On acceptance, the firm will be allocated a dedicated case manager to support in the test's development and implementation. If, however, a firm that is accepted into the sandbox is engaging in regulated activities, then they must apply for the relevant authorisation or registrations.
- The **Digital Sandbox** allows firms to test and develop proofs of concept in a digital testing environment, enabling firms to develop, collaborate, and test new products and solutions. The Digital Sandbox was launched permanently following around 60% of pilots making positive progress, including receipt of funding/partnerships, launching products, and recieving industry rewards and recognitions.
- The **Global Financial Innovation Network** (**GFIN**) is an international network of financial regulators and related organisations committed to supporting financial innovation in the best interests of consumers. The network aims to provide a more efficient way for innovative firms to interact with regulators as the firms look to scale new ideas.
- **TechSprints** form part of the FCA's regulatory toolkit to bring together market participants, including regulators (from across and outside financial services), to collaborate to develop technology-based ideas or proofs of concept to address specific industry challenges. As well as exploring solutions, TechSprints are intended to act as a catalyst for change to help unlock the potential benefits of technology innovation.
- **CryptoSprint** events were held by the FCA in May and June 2022, providing an opportunity to explore potential UK policy solutions for the regulation of cryptoassets. This is the first time that the FCA had gathered views from industry and other stakeholders to help it understand emerging cryptoasset market practices and help shape future policy.

Additionally, in March 2022, the Centre for Finance, Innovation and Technology (the **CFIT**) published terms of reference[16] announcing that the CFIT model will comprise a "coalitions" approach, striving to support the growth of the sector. The CFIT is a virtual body that enables enhanced connectivity across the regions and provides research and data capabilities in financial technology and innovation. The initial work of the CFIT will focus on unlocking datasets to show the potential of open finance in delivering better financial outcomes for small and medium-sized enterprises (**SMEs**) and consumers across the UK.

Under the FSMB, HMT will be granted the power to issue statutory instruments allowing the creation of regulatory "sandboxes" (tools allowing businesses to explore and experiment with new and innovative products, services or businesses under a regulator's supervision).

The government has announced plans to introduce a "financial market infrastructure sandbox" to enable firms to experiment and innovate in providing the infrastructure services that underpin markets, namely by enabling DLT to be tested. This sandbox will be created in the latter half of 2023.

The government has also announced plans to establish a Cryptoasset Engagement Group to work closely with the industry. This would involve the BoE and other key industry figures meeting regularly to discuss the direction of the cryptoasset industry and how best to support its growth.

All the above are part of government's plan to make the UK a global hub for cryptoasset technology, with the measures helping firms to invest, innovate and scale up in the UK.[17] Additionally, and given that the UK has a "second-mover advantage" following the prior implementation of MiCAR, the Consultation also has significant potential to increase innovation within the UK market.[18]

Ownership and licensing requirements

Two key publications are seeking to enhance clarity around digital assets, though they do not purport to change regulatory aspects.

Law Commission – Consultation on Digital Assets

In August 2022, the Law Commission for England and Wales (the **Commission**) launched a detailed consultation[19] that contained reform proposals to better recognise and protect digital assets, especially crypto-tokens.

In June 2023, the Commission issued its final report on digital assets[20] setting out a tripartite approach to addressing the legal uncertainty that remains in the evolving digital asset market.[21] To reduce this residual uncertainty, the Commission recommended law reform to ensure that the current legal system can reinforce the strength of the digital asset ecosystems while ensuring that the private law of England and Wales remains a dynamic, flexible tool that will give UK market participants a global competitive advantage in the space.[22] To achieve this, the Commission's final report: (i) prioritises the development of common law; (ii) proposes targeted statutory reform solely to support the existing common law position or where the further development of common law is not feasible; and (iii) recommends that the UK government create a panel of technical experts, legal practitioners, academics, and judges to provide non-binding guidance.

The Commission's key recommendation from the consultation, as reiterated in the final report, is the explicit recognition of a third category of personal property for "data objects"; this would recognise digital assets as distinct things, capable of being objects of personal property rights. The definition is supplemental to the two existing categories of "things in possession" and "things in action", as digital assets risk falling between the two categories; the Commission recommends express statutory confirmation that a thing will not be deprived of legal status as an object of personal property rights merely by reason of the fact that it is neither a thing of action, nor a thing in possession. To qualify as a data object and attract property rights, a digital asset must:

- be composed of data represented in an electronic medium, including in the form of computer code, electronic, digital, or analogue signals;
- exist independently of persons (who may claim to own them) and the legal system (which could be relied on when trying to enforce rights relating to them); and
- be rivalrous; that is, their use by one person inherently prevents simultaneous use by another person.

Divestibility could then serve as an indicator as to whether a digital asset constitutes a data object if the transfer of the object results in the transferor being deprived of it. The Commission recognises that crypto-tokens and cryptoassets can generally satisfy this criterion.

The Commission also proposed a new concept of control via common law, intending to strike a balance between recognising the unique features of data objects while retaining the benefits of the law of possession. Control would depend on the factual ability to determine whether a person has use over the data object, rather than any legal rights they might possess in relation to it. A person in control of a data object can: exclude others from using it; use and transfer it; and identify themselves as the person able to carry out these rights. However, in accordance with the existing legal concept of possession, there is no requirement of intention. The Commission acknowledges that this concept might not be able to address complex legal mechanisms and arrangements, such as custody and collateral arrangements.

UK Jurisdiction Taskforce – Legal Statement

The Commission's consultation draws on the conclusions of the UK Jurisdiction Taskforce (the **UKJT**) Legal Statement[23] published in 2019 on the Status of Cryptoassets and Smart Contracts, which stated that: (i) cryptoassets are property; (ii) cryptoassets can, at least to some extent, be owned, transferred, assigned, and made the subject of security interests; and (iii) smart contracts are capable of being contracts under English law. This has been adopted and upheld by the High Court of England and Wales when it held that particular cryptoassets were capable of constituting a form of property.[24] In April 2021, the UKJT published its Digital Dispute Resolution Rules,[25] which were to be incorporated into on-chain digital relationships and smart contracts. This established an arbitration regime for settling any disputes relating to cryptoassets, smart contracts, or other novel digital technologies.

In February 2023, the UKJT published a legal statement confirming that English law already supports a range of digital securities structures, without the need for statutory intervention.[26]

Mining

How cryptoassets are "mined" (*i.e.*, the process by which miners are rewarded, if successful, with new units of a particular cryptoasset for completing a specified activity and thus validating and adding transactions to a blockchain) depends on the consensus mechanism adopted by a particular blockchain. For example, transactions are validated on the Bitcoin blockchain via the proof-of-work (**PoW**) consensus mechanism, which requires validators to compete to solve complex mathematical equations.[27]

This was also the case for the Ethereum blockchain until September 2022, when its highly anticipated transition to the proof-of-stake (**PoS**) consensus mechanism took place. During this software upgrade (termed the Ethereum Merge (the **Merge**)), the original execution layer of the Ethereum blockchain merged with a new PoS consensus layer, which subsequently resulted in transactions being validated via a PoS consensus mechanism. As an alternative to the competitive PoW validation method, PoS relies on validators selected at random to confirm transactions and create new blocks. The Merge laid the technical foundation for future scalability improvements on the Ethereum blockchain and was implemented to address some of the issues experienced with PoW: comparatively, the Merge is more secure, less energy-intensive, and has increased throughput. Together, these features have allowed transactions and blocks to be approved more quickly than with PoW. However, the PoS consensus mechanism may potentially give rise to regulatory scrutiny due to the staking component of the process.

With PoS, participating validator nodes operating on a PoS network must stake capital (*i.e.*, tokens) into a smart contract on the network to be eligible to validate transactions. Notwithstanding PoS validator nodes being selected at random, they have an increased likelihood of being selected to validate by virtue of having a large number of tokens staked in the deposit contract (*e.g.*, to participate as a validator, a user must stake 32 ETH). These tokens represent value "put at stake" that can be destroyed if the validator acts dishonestly when reviewing, proposing, and sending blocks.[28] Recognising the profitability of staking, service providers have emerged that offer customers the option to stake their tokens to the service provider's validator node, thereby increasing their chances of being selected to validate new blocks and subsequently earn staking rewards, which are then passed on to customers in proportion to their tokens staked (**Validator Service Providers**).

Staking activities via Validator Service Providers may fall within the definition of a collective investment scheme (**CIS**) pursuant to section 235 of FSMA. For example, it may be argued that this activity constitutes a CIS if: (i) participants do not have day-to-day control over the management of cryptoassets staked with a validator node; (ii) participants' assets are pooled together by the validator nodes; (iii) a participant has an expectation of profits by way of their participation in the staking process; and (iv) the staked cryptoassets are managed by the Validator Service Provider as operator of the scheme. Notwithstanding the foregoing, each project will likely be assessed on a case-by-case basis as there are additional elements to the CIS definition that may or may not be satisfied depending on a particular project's mechanics. The relationship between staking and the definition of a CIS has not yet been tested.

HMT has noted that there may not be a justification to regulate the activity of mining in and of itself; however, it has questioned industry participants as to whether other regulatory outcomes should be pursued in regulating mining (*e.g.*, "miner extractable value", whereby miners select how to sequence transactions to extract value from other traders). Accordingly, the mining and staking of cryptoassets fall outside of the existing regulatory perimeter and are not expressly regulated activities in the UK (apart from HMRC considering any profits derived from mining activities to be taxable for individuals and businesses either as trading profits or under the miscellaneous income provisions).

Border restrictions and declaration

Upon arrival in the UK, individuals carrying £10,000 or more in cash must declare this fact to HMRC on a customs declaration form. At the time of this writing, there are no express border restrictions against transporting cryptoassets into the UK for personal or investment purposes provided any applicable customs and declaration requirements are adhered to. HMRC does not consider cryptoassets to constitute currency or money; however, there is a possibility that a declaration of cryptoasset holdings upon re-entry into the UK would be required if it is determined that a cryptoasset constitutes a "good", as cryptoassets are subject to tax reporting obligations.[29]

Reporting requirements

Reporting requirements contained in financial regulation or AML legislation may apply in relation to cryptocurrency transactions. The MLRs also contain a broad reporting requirement applicable to CEPs and CWPs, which means that they must produce information that the FCA requires relating to their compliance with the MLRs.

Estate planning and testamentary succession

HMRC has confirmed that it considers cryptoassets to be property for the purposes of inheritance tax. UK-domiciled (or deemed domiciled) individuals (for tax purposes) are subject to UK inheritance tax on their worldwide estates. As such, cryptoassets will form part of the individual's estate and will be subject to the standard inheritance tax rate of 40% (assuming the value of the estate exceeds the £325,000 tax-free threshold). The taxable amount on the cryptoasset(s) will be calculated on the individual's death. Executors cannot claim for any rebate on crypoassets. Non-UK-domiciled individuals are, subject to exceptions, subject to taxation of any assets held and situated in the UK.

A testator should instruct their personal representative on how to acquire the cryptographic keys and details of wallet service providers, otherwise the value of cryptoassets left to beneficiaries of an estate will be lost.

* * *

Endnotes

1. Regulators in the UK prefer the term "cryptoasset", rather than "cryptocurrencies", as it captures a broader range of tokens than just those intended to operate as a means of exchange. These terms may be used interchangeably, as well as terms such as "virtual asset", "virtual currency", "digital asset" and "digital currency".
2. Financial Services and Markets Act 2000 (Financial Promotion) (Amendment) Order 2023.
3. https://www.fca.org.uk/publication/policy/ps23-6.pdf
4. https://www.fca.org.uk/publication/policy/ps22-10.pdf
5. Chapter 5 of the Consultation.
6. Government sets out plan to make UK a global cryptoasset technology hub | GOV.UK (https://www.gov.uk).
7. The taxation of decentralised finance (DeFi) involving the lending and staking of cryptoassets | GOV.UK (https://www.gov.uk).
8. The Investment Manager (Investment Transactions) (Cryptoassets) Regulations 2022 (publishing.service.gov.uk).
9. The taxation of decentralised finance (DeFi) involving the lending and staking of cryptoassets | GOV.UK (https://www.gov.uk).
10. International Standards for Automatic Exchange of Information in Tax Matters: Crypto-Asset Reporting Framework and 2023 update to the Common Reporting Standard | en | OECD.
11. CRYPTO20000 – Cryptoassets for individuals: contents – HMRC internal manual | GOV.UK (https://www.gov.uk).
12. CRYPTO40000 – Cryptoassets for businesses: contents – HMRC internal manual | GOV.UK (https://www.gov.uk).
13. HM Revenue & Customs, *Money laundering supervision for money laundering businesses*, GOV.UK, https://www.gov.uk/guidance/money-laundering-regulations-money-service-business-registration#registering-with-the-financial-conduct-authority
14. HM Revenue & Customs, *Money service business guidance for money laundering supervision*, GOV.UK, https://www.gov.uk/government/publications/anti-money-laundering-guidance-for-money-service-businesses (last visited Aug. 5, 2023).

15. HM Treasury, *Future financial services regulatory regime for cryptoassets: consultation and call for evidence*, at 18 (2023).
16. Terms of Reference: March 2022 – Centre for Finance, Innovation and Technology Steering Committee | GOV.UK (https://www.gov.uk).
17. Government sets out plan to make UK a global cryptoasset technology hub | GOV.UK (https://www.gov.uk).
18. UK Crypto Asset Regulation Should 'Increase Economic Competitiveness' and 'Innovation', Urges Acuiti | *The Fintech Times*.
19. Law Commission Documents Template.
20. Note that the Law Commission describes cryptoassets as digital assets.
21. Law Commission, Digital Assets: Final Report, HC1486, Law Com. No. 412, https://s3-eu-west-2.amazonaws.com/lawcom-prod-storage-11jsxou24uy7q/uploads/2023/06/Final-digital-assets-report-FOR-WEBSITE-2.pdf
22. Law Commission, Digital Assets: Summary of Final Report, https://s3-eu-west-2.amazonaws.com/lawcom-prod-storage-11jsxou24uy7q/uploads/2023/06/14.294_LC_Digital-assets-summary_v5_WEB.pdf
23. Legal statement on cryptoassets and smart contracts (https://lawtechuk.io).
24. *AA v Persons Unknown & Ors, Re Bitcoin* [2019] EWHC 3556 (Comm) (13 December 2019) (https://www.bailii.org/cgi-bin/format.cgi?doc=/ew/cases/EWHC/Comm/2019/3556.html&query=(.2019.)+AND+(EWHC)+AND+(3556)+AND+((Comm))+AND+((13)+AND+(December)+AND+(2019)).
25. 2. UKJT Digital Disupte Rules.pdf (https://lawtechuk.io).
26. https://ukjt.lawtechuk.io (last visited Aug. 5, 2023).
27. What Is Cryptocurrency Mining? | Binance Academy (https://academy.binance.com/en/articles/what-is-cryptocurrency-mining).
28. @corwintines, *Proof-of-Stake (PoS)*, Ethereum.org, https://ethereum.org/en/developers/docs/consensus-mechanisms/pos (last visited Aug. 5, 2023).
29. *Check if you need to declare goods you bring into or take out of the UK*, GOV.UK, https://www.tax.service.gov.uk/guidance/check-if-you-need-to-declare-goods-you-bring-into-or-take-out-of-the-UK/outcome/another-gb-personal-travelling-may-need-to-declare (last visited Aug. 5, 2023).

* * *

Acknowledgment

The authors would like to thank Yao An Chua for his contribution to the Taxation section of this chapter.

Charles Kerrigan
Tel: +44 20 7067 3437 / Email: charles.kerrigan@cms-cmno.com
The Blockchain Industry in the UK Landscape Overview names Charles as a "leading influencer". He is part of teams working on investing and setting standards for emtech in the UK, Europe and the US.
Charles is a specialist in emerging technologies including crypto, digital assets, decentralised finance and AI. He works on corporate finance and venture capital fundraising transactions for companies, funds, platforms, and financial institutions, as well as consulting projects on blockchain, AI and automation/transformation for public bodies, policymakers, standards institutions, and corporations.

Christina Fraziero
Tel: +44 20 7067 3406 / Email: christina.fraziero@cms-cmno.com
Christina Fraziero is a lawyer at CMS London and a member of the firm's Crypto & Digital Assets team where she advises a range of high-profile industry participants on cryptoasset activities, DeFi, NFTs, fundraising, and decentralised protocol governance. Christina has been working with startup and scale-up Web3 clients in an advisory capacity, both in the US and the UK. Prior to joining CMS, Christina worked in-house at the US's preeminent securities market regulator, a global cryptoasset exchchange, a venture capital studio, and the group of software development companies that created the largest DeFi liquidity protocol in Europe.

Olivia Hamilton-Russell
Tel: +44 20 7067 3476 / Email: olivia.hamilton-russell@cms-cmno.com
Olivia Hamilton-Russell is a lawyer at CMS London. As part of the Crypto & Digital Assets team, she works on a range of crypto- and blockchain-related matters for a range of high-profile industry participants. Her experience includes work relating to token and equity fundraising via SAFTs, SAFTEs and token warrants, as well as advising on regulatory and commercial matters for crypto businesses and their corresponding native tokens. Olivia has significant experience advising in respect of funds and finance transactions at top-tier law firms. Prior to joining CMS, Olivia was a programme manager at a global Web3 accelerator.

Antonia Bain
Tel: +44 131 200 7529/ Email: antonia.bain@cms-cmno.com
Antonia Bain is a paralegal based in CMS Edinburgh, currently training before qualifying as a solicitor. Prior to joining CMS, she graduated from the University of Edinburgh in 2021 with a First Class Law LL.B. (Hons) and obtained a Distinction in her LL.M. in Commercial Law in 2022. She won the prize for most distinguished scholar across all LL.M. programmes at the university, where she was writing on various aspects of corporate finance, including insolvencies in corporate groups and equity-sourced crowdfunding via fintech platforms. Antonia was recently involved in producing a multijurisdictional guide to cryptoasset regulations.

CMS LLP

Cannon Place, 78 Cannon Street, London EC4N 6AF, United Kingdom
Tel: +44 207 367 3000 / URL: www.cms.law

USA

Josias N. Dewey & Samir Patel
Holland & Knight LLP

Government attitude and definition

In the United States, cryptocurrencies have been the focus of much attention by both federal and state governments. At the federal level, most of the focus has been at the administrative and agency level, including the Securities and Exchange Commission (the "**SEC**"), the Commodity Futures Trading Commission (the "**CFTC**"), the Federal Trade Commission (the "**FTC**") and the Department of the Treasury (the "**Treasury**"), through the Internal Revenue Service (the "**IRS**"), the Office of the Comptroller of the Currency (the "**OCC**") and the Financial Crimes Enforcement Network ("**FinCEN**"). While there has been significant engagement by these agencies, little formal rulemaking has occurred. Many federal agencies and policymakers have praised the technology as being an important part of the U.S.'s future infrastructure and have acknowledged the need for the U.S. to maintain a leading role in the development of the technology.

Beginning in 2022, and coinciding with the proliferation of cryptocurrencies in mainstream society, U.S. Congress has introduced several bills aimed at providing more clarity to the emerging sector. The bipartisan introduced Responsible Financial Innovation Act (the "**RFIA**") was designed to provide regulatory clarity for agencies charged with supervising digital asset markets, provide a strong, tailored regulatory framework for stablecoins, integrate digital assets into existing tax and banking law and spur innovation in the field of digital assets.

Democratic Senator Patrick Toomey introduced a bill that would create a regulatory framework for stablecoins and their issues, currently known as the Toomey Stablecoin Bill. This bill includes authorizing three options for the issuance of payment stablecoins (national limited payment stablecoin issuers, insured depository institutions and money transmitting businesses), subjecting all payment stablecoin issuers to standardized requirements, distinguishing stablecoins from securities by indicating that, at a minimum, stablecoins that do not offer interest are not securities, and applying privacy protections to transactions involving stablecoins and other virtual currencies.

In the second half of 2022, bipartisan senators introduced the Digital Commodities Consumer Protection Act (the "**DCCPA**"), authorizing the CFTC to regulate "digital commodity platforms" and "digital commodity" trading. The DCCPA would give the CFTC exclusive jurisdiction over "digital commodity" trades, except transactions in which a merchant or consumer is using a digital commodity solely for the purchase or sale of a good or service. "Digital commodity" was defined as a fungible digital form of personal property that can be possessed and transferred person-to-person without necessary reliance on an intermediary.

Two months later, Republican Senator Bill Hagerty introduced the Digital Trading Clarity Act, which provides that a digital asset not subject to a determination by the SEC or a federal court, and listed through an intermediary that meets certain requirements related to custody,

disclosure, and other investor protections, would not be considered a security. In July of 2023, an updated version of the RFIA was introduced, aimed at providing greater consumer protections amid a cascading contagion of bankruptcies among blockchain companies and stakeholders. Eight days later, House Representatives Patrick McHenry, Chairman of the House Financial Services Committee, and Glenn Thompson, Chairman of the House Committee on Agriculture, introduced the Financial Innovation and Technology for the 21st Century Act (the "**McHenry-Thompson Bill**"), which provides a statutory framework for digital asset regulation intended to provide clarity and fill regulatory gaps. Both the House and Senate bills seek to integrate the regulation of digital assets and digital asset derivatives into the existing U.S. regulatory framework – primarily that of the SEC and CFTC – rather than create a standalone framework, discussed further below.

Many state governments have proposed and/or passed laws affecting cryptocurrencies and blockchain technology, with most of the activity taking place in the legislative branch. There have generally been two approaches to regulation at the state level. Some states have tried to promote the technology by passing very favorable regulations exempting cryptocurrencies from state securities laws and/or money transmission statutes. These states hope to leverage investment in the technology to stimulate local economies and improve public services. One example, Wyoming, has been mentioned as a state seeking a broader impact on its economy. In furtherance of this objective, Wyoming passed legislation allowing for the creation of a new type of bank or special purpose depository institution. These crypto-focused banks can act in both a custodial and fiduciary capacity and are meant to allow businesses to hold digital assets safely and legally. The state also passed legislation aimed at easing the formation of decentralized autonomous organizations ("**DAOs**"). By issuing the DAO Supplemental Bill, Wyoming became the first state to regulate DAOs and to recognize them as a form of limited liability company ("**LLC**"). In its most ambitious endeavor yet, the state enacted the Wyoming Stable Token Act. This act creates a path for Wyoming to issue the U.S.'s first government-issued stablecoin, which would be fully backed by reserves of U.S. dollars. Neighboring Utah is following in Wyoming's footsteps by enacting its own Decentralized Autonomous Organizational Act, which allows DAOs that are not registered as a for-profit corporate entity or a non-profit entity to be treated as the legal equivalent of a domestic LLC. This came after Utah allowed payments to government agencies to be made with digital assets. In what many viewed as a surprise, the governor of California vetoed the proposed Digital Financial Assets Law, which would have prohibited exchanges and other parties from digital financial asset business activity unless licensed with the state's Department of Financial Protection and Innovation.

Yet conversely, a growing number of states are making it harder for blockchain companies to operate within their borders by requiring money transmitter licenses and/or the need to strictly adhere to state blue sky securities laws. Within the past year, a number of states, including Florida, and the District of Columbia amended their money transmitter regulations to include virtual currencies/cryptocurrencies and requiring certain intermediaries to have a state-issued license. This past year also saw the rise of multistate coalitions protecting their state securities laws against some of the biggest companies in the blockchain space. On June 6, 2023, following an investigation by a task force of nine states, including California and New York, and with assistance from the SEC, each state filed enforcement actions against cryptocurrency exchange Coinbase and its parent corporation alleging that Coinbase's staking rewards program constituted unregistered securities sales in violation of state securities laws. Another five state coalitions filed cease-and-desist orders against Nexo Inc., alleging that Nexo violated their state blue sky laws by offering unregistered securities

within their state. On January 19, 2023, Nexo settled with the multistate coalitions for $22.5 million in the aggregate. A clear pattern is emerging, mirroring other industries, where bigger states with bigger economies clearly intend to regulate blockchain technology, whereas smaller states seek to be a regulatory refuge for blockchain stakeholders.

There is no uniform definition of "cryptocurrency," which is often referred to as "virtual currency," "digital assets," "digital tokens," "cryptoassets" or simply "crypto." The Uniform Law Commission and the American Law Institute amended the Uniform Commercial Code to include Article 12, which defines and governs digital assets specifically. The new article includes virtual currencies in its definition of "controllable electronic records." Several states have already adopted the amendment. Other jurisdictions have attempted to formulate a detailed definition for the asset class, most have wisely opted for broader, more technology-agnostic definitions. Those taking the latter approach will be better positioned to regulate as and when the technology evolves.

The Biden Administration released an Executive Order ("**EO**") outlining an approach to address risks stemming from the growth of digital assets and blockchain technology while supporting responsible innovation. The EO focuses on six key priorities: (1) consumer and investor protection; (2) financial stability; (3) illicit finance; (4) U.S. leadership in the global financial system and economic competitiveness; (5) financial inclusion; and (6) responsible innovation.

To advance these key priorities, the EO called for a number of reports, studies and plans, including reports from the Treasury, on: (1) the future of money and potential impacts of a U.S. central bank digital currency ("**CBDC**"); and (2) policy recommendations around consumer protection and financial inclusion issues. It also calls for the Financial Stability Oversight Council to produce a report on financial stability risks and regulatory gaps. In response to the EO, the White House released a fact sheet designed to provide a comprehensive framework for regulating digital assets based on input from various U.S. government agencies and departments. The framework greenlights regulators such as the SEC and CFTC to continue coordinating efforts to enforce law in the industry and to share data on consumer complaints in the space. The Treasury will take an active role in working with financial institutions to help identify and mitigate cyber risks through data sharing and analysis. It is also tasked with working with regulators to ensure that crypto firms have regulatory guidance. The fact sheet also mentions a potential U.S. CBDC, citing many potential benefits in technology, the economy, security and individual liberty.

On March 20, 2023, the White House published the 2023 Economic Report of the President, which, for the first time, includes an entire 35-page chapter on digital assets. It provides a number of pointed criticisms of cryptocurrency – an apparent shift from the previous approach of the Biden Administration articulated in the EO.

The report states that cryptoassets currently do not offer widespread economic benefit. Additionally, the report claims that cryptoassets are mainly a speculative investment vehicle and not an effective alternative to fiat currency. It acknowledged that some cryptoassets are here to stay, and states that much of the activity in the cryptoasset space is covered by existing regulations.

Sales regulation

The sale of cryptocurrency is generally only regulated if the sale (i) constitutes the sale of a security under state or federal law, or (ii) is considered money transmission under state law or conduct otherwise making the person a money services business ("**MSB**")

under federal law. In addition, futures, options, swaps and other derivative contracts that make reference to the price of a cryptoasset that constitutes a commodity are subject to regulation by the CFTC under the Commodity Exchange Act (the "**CEA**"). In addition, the CFTC has jurisdiction over attempts to engage in market manipulation with respect to those cryptoassets that are considered commodities. For example, the CFTC filed a civil enforcement action in the U.S. District Court for the Southern District of New York charging Avraham Eisenberg with unlawfully misappropriating over $110 million in digital assets from Mango Markets, a purported decentralized digital asset exchange, through "oracle manipulation" in the CFTC's first enforcement action for a fraudulent or manipulative scheme involving trading on a supposed decentralized digital asset platform and the first involving "oracle manipulation."

Securities laws

The SEC generally has regulatory authority over the issuance or resale of any token or other digital asset that constitutes a security. Under U.S. law, a security includes "an investment contract," which has been defined by the U.S. Supreme Court as an investment of money in a common enterprise with a reasonable expectation of profits to be derived from the entrepreneurial or managerial efforts of others. *SEC v. W.J. Howey Co.*, 328 U.S. 293, 301 (1946).

In determining whether a token or other digital asset is an "investment contract," both the SEC and the courts look at the substance of the transaction, instead of its form. In 1943, the U.S. Supreme Court determined that "the reach of the [Securities] Act does not stop with the obvious and commonplace. Novel, uncommon, or irregular devices, whatever they appear to be, are also reached if it be proved as matter of fact that they were widely offered or dealt in under terms or courses of dealing which established their character in commerce as 'investment contracts,' or as 'any interest or instrument commonly known as a 'security'." *SEC v. C.M. Joiner Leasing Corp.*, 320 U.S. 344, 351 (1943). It has also been said that "Congress' purpose in enacting the securities laws was to regulate investments, in whatever form they are made and by whatever name they are called." *Reves v. Ernst & Young*, 494 U.S. 56, 61 (1990).

The SEC has been clear on its position that even if a token issued in an initial coin offering ("**ICO**") has "utility," the token will still be deemed to be a security that is regulated under the Securities Act if it meets elements of the *Howey* test. On February 6, 2018, in written testimony to the U.S. Senate Banking Committee, the Chairman of the SEC stated as follows:

> Certain market professionals have attempted to highlight the utility or voucher-like characteristics of their proposed ICOs in an effort to claim that their proposed tokens or coins are not securities. Many of these assertions that the federal securities laws do not apply to a particular ICO appear to elevate form over substance. The rise of these form-based arguments is a disturbing trend that deprives investors of mandatory protections that clearly are required as a result of the structure of the transaction. Merely calling a token a 'utility' token or structuring it to provide some utility does not prevent the token from being a security.

In a more nuanced speech delivered in June 2018, William Hinman, the SEC's Director of Corporate Finance, stated:

> Returning to the ICOs I am seeing, strictly speaking, the token – or coin or whatever the digital information packet is called – all by itself is not a security, just as the orange groves in *Howey* were not. Central to determining whether a security is being sold is

how it is being sold and the reasonable expectations of purchasers. When someone buys a housing unit to live in, it is probably not a security. But under certain circumstances, the same asset can be offered and sold in a way that causes investors to have a reasonable expectation of profits based on the efforts of others. For example, if the housing unit is offered with a management contract or other services, it can be a security.

Later in the same speech, Mr. Hinman made clear that a digital token that might initially be sold in a transaction, constituting the sale of a security, might thereafter be sold as a non-security where the facts and circumstances have changed over time, such that the *Howey* test is no longer met, specifically, if the blockchain protocol becomes truly decentralized like Bitcoin and Ethereum; negating the "efforts of others" prong of *Howey*. While such comments are not official policy of the SEC, they are a good indicator of it. If a digital asset is determined to be a security, then the issuer must register the security with the SEC or offer it pursuant to an exemption from the registration requirements. For offerings that are being made under a federal exemption from securities registration, the SEC places fewer restrictions on the sale of securities to "accredited investors." An individual investor is an "accredited investor" only if he or she (i) is a director or executive officer of the company issuing the securities, (ii) has an individual net worth (or joint net worth with a spouse) that exceeds $1 million, excluding the value of the investor's primary residence, (iii) has an individual income that exceeds $200,000 in each of the two most recent years, and has a reasonable expectation of reaching the same individual income level in the current year, or (iv) has a joint income that exceeds $300,000 in each of the two most recent years, and has a reasonable expectation of reaching the same joint income level in the current year. See SEC Rule 501(a)(5). Significant enforcement actions by the SEC have included actions brought against Telegram and Kik. These actions highlight the SEC's willingness to aggressively enforce U.S. securities laws in cases involving digital assets. In October 2019, the SEC filed a complaint against Telegram alleging that the company had raised $1.7 billion through the sale of 2.9 billion GRAMS (the company's native cryptocurrency) to finance its business. GRAMS were to allow customers of the messaging service to use the token as a means of payment for goods and services within the Telegram ecosystem. The SEC sought to enjoin Telegram from delivering the GRAMS it sold, which, using the *Howey* test, the regulator alleged were securities and were not properly registered. In March of 2020, the U.S. District Court for the Southern District of New York ("**SDNY**") issued a preliminary injunction. The SEC argued that the Simple Agreement for Future Tokens ("**SAFT**") – mirrored after the commonly used Simple Agreement for Future Equity – and the subsequent resale of GRAMS delivered pursuant to the SAFT, could not be viewed as two isolated phases, but rather should be viewed holistically as a single integrated scheme to issue securities that yield a profit. Ultimately, Telegram abandoned its plan to issue the GRAMS tokens, and agreed to repay the $1.2 billion to investors and pay an $18.5 million civil penalty. The SEC's position could make it more difficult for token issuers to bifurcate between capital-raising activities and the *bona fide* sale of tokens intended to provide some utility other than as an investment.

In October 2020, a federal district court entered a final judgment against Kik Interactive Inc. ("**Kik**") relating to Kik's unregistered offering of digital "Kin" tokens in 2017, which the SEC argued violated U.S. securities laws. More specifically, the SEC alleged that Kik sold securities to U.S. investors without a valid registration as required under U.S. securities laws. The court found that sales of "Kin" tokens constituted investment contracts; and hence, were securities. Kik had argued that its private sales were limited to accredited investors, but the court held that even those sales did not qualify for an exemption because its private and public sales were a single integrated offering. As part of the final judgment, Kik agreed to pay a $5 million penalty.

In December 2020, the SEC announced that it filed an action in the SDNY against Ripple Labs, Inc., alleging that it raised over $1.3 billion through an ongoing unregistered digital asset securities offering. The complaint alleged that Ripple raised funds, beginning in 2013, through the sale of the XRP digital coin in an unregistered securities offering to investors in the U.S. After the SEC's announcement, most major U.S. crypto exchanges, including Coinbase, delisted or halted trading of XRP. However, defendants maintained their assertion that XRP is a cryptocurrency and does not need to be registered as an investment contract. In March 2022, the SDNY denied the SEC's motion to strike Ripple's "fair notice" defense. Ripple asserted that the SEC failed to provide Ripple with fair notice that its unregistered sales of XRP violated federal law. Among other things, Ripple asserted that the SEC failed to take action in 2015 when Ripple reached a settlement with the U.S. Department of Justice ("**DOJ**") and the Treasury's FinCEN, which described XRP as a "convertible virtual currency," permitting future sales of XRP subject to laws and regulations applicable to MSBs.

On July 13, 2023, the court issued its order granting in part and denying in part cross motions for summary judgment filed by both parties, holding that, under the *Howey* test, unregistered sales of XRP to retail investors on digital asset exchanges did not constitute the offer and sale of cryptoasset securities under the U.S. securities laws, while sales of XRP to institutional investors were prohibited offers and sales. The court held that *programmatic sales* of XRP to retail investors on digital asset exchanges did not constitute the offer and sale of securities because these sales were blind bid/ask transactions and retail buyers could not have known whether their payments of money went to Ripple or another unaffiliated intermediary. Sales of XRP to institutional investors did constitute the offer and sale of securities because institutional investors would have purchased XRP with the expectation that they would derive profits from Ripple's efforts, and Ripple led institutional investors to believe it would use the capital received from its institutional sales to improve the market for XRP and develop uses for the XRP ledger, thereby increasing the value of XRP. However, this ruling was quickly challenged by another judge sitting on the same bench.

In another complaint filed in the same SDNY, the SEC charged Singapore-based Terraform Labs ("**Terraform**"), with violating SEC registration and anti-fraud provisions by orchestrating a multi-billion dollar cryptoasset securities fraud involving tokens that the SEC asserted were security-based swaps, designed to pay returns by mirroring stock prices of U.S. companies, and Terra USD ("**UST**"), an "algorithmic" stablecoin that supposedly maintained its U.S. dollar peg by being interchangeable for LUNA coin, another of the cryptoasset securities issued by Terraform. Terraform tried to take advantage of the *Ripple* case ruling and filed a motion for the dismissal of the suit using Ripple's victory as an argument. In denying Terraform's dismissal, the judge rejected to consider the categorization of sales used in the *Ripple* case, stating:

> It may also be mentioned that the Court declines to draw a distinction between these coins based on their manner of sale, such that coins sold directly to institutional investors are considered securities and those sold through secondary market transactions to retail investors are not. In doing so, the Court rejects the approach recently adopted by another judge of this District in a similar case[.]
>
> Simply put, secondary market purchasers had every bit as good a reason to believe that the defendants would take their capital contributions and use it to generate profits on their behalf.

Note that the *Terraform* decision must be considered in the context of the defendants' motion to dismiss, and the court's obligation in determining such a motion, generally, to

consider all allegations of the SEC as true. The *Ripple* decision, by contrast, came on cross-motions for summary judgment after extensive fact and expert discovery had occurred. The *Terraform* case will proceed to the discovery phase.

The outcomes of the Telegram, Kik and Ripple Labs proceedings make it incredibly difficult to consummate most token-generating events involving U.S. persons. Many issuers have opted to exclude U.S. persons from token offerings, and instead have elected to limit sales to non-U.S. persons (e.g., pursuant to the Regulation S safe harbor).

Two other implications for a token constituting a security are (i) the requirement that a person be a broker-dealer licensed with the SEC and a member of the Financial Industry Regulatory Authority ("**FINRA**") in order to facilitate the sale of securities or to act as a market maker or otherwise constitute a dealer in the asset, and (ii) the asset can only trade on a licensed securities exchange or alternative trading system ("**ATS**") approved by the SEC. Several exchanges attained approval as an ATS and several firms have been registered as a broker-dealer, in each case, with the intent to deal in cryptocurrencies that are considered securities. To date, however, there are only a handful of security tokens actively trading on these ATS platforms.

This is likely the result of the difficulties in integrating traditional securities laws around the transfer of securities and the notion of a peer-to-peer network that seeks to operate without intermediaries.

In an attempt to harmonize securities laws with blockchain technology, the SEC has proposed two amendments to the Exchange Act, redefining the terms "exchange" and "dealer." In January 2022, the SEC the proposed amendments to Rule 3b-16 and the term "exchanges:"

- exchanges are defined in terms of buyers and sellers with trading interest as opposed to orders;
- exchanges include organizations, associations, or groups of persons that simply make available – rather than use – established, non-discretionary methods that allow for interaction and agreement on the terms of trades; and
- exchanges include not only organizations, associations, or groups of persons that provide trading facilities or set rules, but also organizations, associations, or groups of persons that merely provide communication protocols.

These proposed amendments, which deformalize the criteria for being an exchange, have clear and potentially profound implications for decentralized finance ("**DeFi**"). Under the proposed definition of exchange, an organization, association, or group of persons that passively makes available a communication protocol under which buyers and sellers with trading interest can interact and agree on the terms of trades is an exchange.

In March 2022, the SEC proposed rules that would greatly expand the Exchange Act definition of "dealer" and essentially kill the distinction between dealers and traders long recognized by the SEC. The likely outcome is that most proprietary trading firms will need to register with the SEC as dealers and become members of FINRA or a national securities exchange. The SEC's focus is on "market participants who engage in a routine pattern of buying and selling securities for their own account that has the effect of providing liquidity." The proposed qualitative standards are below, any one of which would be sufficient to push what today is viewed as a non-registered trading to the category of registered (and regulated) dealer activity "regardless of whether the liquidity provision is a chosen consequence the activity:"

- routinely making roughly comparable purchases and sales of the same or substantially similar securities in a day;

- routinely expressing trading interests that are at or near the best available prices on both sides of the market and that are communicated and represented in a way that makes them accessible to other market participants; or
- earning revenue primarily from capturing bid-ask spreads, by buying at the bid and selling at the offer, or from capturing any incentives offered by trading venues to liquidity-supplying trading interests.

In addition to covering proprietary traders in equities, fixed income, and other traditional financial assets, the proposal may lead to a dealer registration requirement for automated market makers and other liquidity providers in the cryptocurrency and DeFi space. Between the exchange and dealer proposals, a staggering number of companies and software developers in the crypto and DeFi space may become subject to the SEC's broker-dealer framework, including registration with the SEC and FINRA membership. In a certain way, this outcome would be consistent with SEC's long-enunciated approach that it will employ the existing laws and regulatory framework to new technologies.

Proving a viable path towards registration and membership, on May 17, 2023, Prometheum Ember Capital LLC ("**Prometheum**") received approval from FINRA to operate as a special purpose broker-dealer ("**SPBD**") for digital assets. Prometheum is the first SPBD allowed to operate as a broker-dealer and as a qualified custodian in the U.S. This approval follows guidance issued by the SEC permitting an SPBD to custody digital assets so long as it complies with Securities Exchange Act Rule 15c3-3 (the Customer Protection Rule). This SPBD addresses the lack of investor protection in the digital assets space by offering both retail and institutional investors an opportunity to custody their digital assets with an SEC-registered SPBD and a FINRA member firm.

SEC v. CFTC oversight of digital assets

In July 2022, the DOJ and the SEC each brought insider trading charges against a former Coinbase product manager for using material non-public information to purchase a variety of cryptoassets prior to announcements by Coinbase that the assets would be listed on the company's platform.

The SEC's allegation that the product manager violated Section 10(b) and Rule 10b-5 of the Exchange Act requires that the tokens traded were securities. Significantly, while the SEC alleges that the manager used material, non-public information to purchase 25 different digital assets ahead of listing announcements, the complaint only alleges that nine of the assets were securities. The other 16 are not even identified, let alone alleged to be securities. Coinbase has strongly challenged the notion that any of the cryptoassets on its platform are securities.

In response to the SEC complaint, CFTC Commissioner Caroline Pham issued an unusually harsh statement criticizing the SEC's approach. Commissioner Pham states she comes to a different view than the SEC on whether utility and governance tokens are securities. Specifically, she notes that: "The SEC complaint alleges that dozens of digital assets, including those that could be described as utility tokens and/or certain tokens relating to DAOs, are securities."

Commissioner Pham also urged the CFTC to take a leading role in this space, which highlights the tension between the SEC and CFTC as to who should regulate digital assets.

In an effort to harmonize digital asset regulation, the proposed Digital Trading Clarity Act aims to provide regulatory clarity around two primary concerns plaguing crypto exchange establishments: (i) the classification of digital assets; and (ii) related liabilities under existing securities laws. If determined by a federal court through a final judgment, or the

SEC through formal rulemaking or enforcement action, and without objection from the CFTC, that a digital asset is a security, the bill requires the SEC Division of Examinations to request information from an intermediary listing that asset to determine whether the intermediary meets the requirements in the bill text. If it does, the intermediary and digital asset enter into a two-year "compliance period" in which the intermediary would not be subject to enforcement actions for listing that asset or failing to register as a national securities exchange or broker-dealer in connection with that asset.

In September 2022, SEC Chair Gary Gensler indicated in a speech at a Practising Law Institute SEC Speaks event, and again on September 15, 2022 in congressional testimony, that certain crypto intermediaries must register with the SEC. Gensler also offered support for CFTC regulation of "non-security" tokens.

In July 2023, an updated version of the RFIA – first introduced in 2022 – attempts to codify a clear regulatory framework for which cryptoassets are securities or commodities. Under the RFIA, the CFTC would have exclusive jurisdiction over a crypto token that qualifies as an ancillary asset but not the "security that constitutes an investment contract." To qualify as an ancillary asset, the token must not offer the holder any financial rights in a business, such as to debt or equity, liquidation, or interest or dividend payments. The SEC, however, would have a role to play: where the average daily aggregate value of transactions in the ancillary asset exceeds a certain threshold, and where the issuer engaged in "entrepreneurial or managerial efforts that primarily determined the value of the ancillary asset," the issuer would be required to file detailed disclosures with the SEC.

In the same vein, the McHenry-Thompson Bill gives the CFTC primary jurisdiction over digital asset markets but details a process for market participants and regulators to follow in allocating oversight of digital assets between the SEC and CFTC. A digital asset is classified as a "digital commodity" and is regulated by the CFTC if the blockchain network to which a digital asset relates is both "functional" and certified as "decentralized." Any person (whether or not related to the network's development) may certify an asset's status as a digital commodity. Networks are presumed decentralized unless the SEC objects within 30 days of the certification and provides a detailed analysis of its reasons for doing so. The SEC would regulate "restricted digital assets," which are: (i) digital assets held by the issuer of the digital asset or affiliates before the networks to which the assets relate are functional and certified as decentralized (known as a premining); and (ii) digital assets held by persons other than issuers or affiliates before the networks to which the assets relate are functional and certified as decentralized, unless the digital assets are distributed through an "end user distribution" or acquired on a CFTC-regulated exchange. In response to the *Ripple* decision, both Republican and Democratic members of Congress sent letters to the SEC, urging the agency to reassess its strategy. If the courts rule against the SEC in other cases, as occurred in *Terraform*, Congress might feel more urgency to enact legislation to resolve legal ambiguities between administrative agencies.

Money transmission laws and anti-money laundering requirements

Under the Bank Secrecy Act (the "**BSA**"), FinCEN regulates MSBs. On March 18, 2013, FinCEN issued guidance that stated the following would be considered MSBs: (i) a virtual currency exchange; and (ii) an administrator of a centralized repository of virtual currency who has the authority to both issue and redeem the virtual currency. FinCEN issued guidance that stated as follows: "An administrator or exchanger that (1) accepts and transmits a convertible virtual currency or (2) buys or sells convertible virtual currency for any reason is

a money transmitter under FinCEN's regulations, unless a limitation to or exemption from the definition applies to the person." See FIN-2013-G001, Application of FinCEN's Regulations to Persons Administering, Exchanging or Using Virtual Currencies (March 18, 2013).

An MSB that is money transmitter must conduct a comprehensive risk assessment of its exposure to money laundering and implement an anti-money laundering ("**AML**") program based on such risk assessment. FinCEN regulations require MSBs to develop, implement, and maintain a written program that is reasonably designed to prevent the MSB from being used to facilitate money laundering and the financing of terrorist activities. The AML program must: (i) incorporate written policies, procedures and internal controls reasonably designed to assure ongoing compliance; (ii) designate an individual compliance officer responsible for assuring day-to-day compliance with the program and BSA requirements; (iii) provide training for appropriate personnel, which specifically includes training in the detection of suspicious transactions; and (iv) provide for independent review to monitor and maintain an adequate program.

All U.S. persons are prohibited from doing business with foreign nationals who are on the Specially Designated Nationals and Blocked Entities List ("**SDN List**") of the Treasury's Office of Foreign Assets Control ("**OFAC**"). OFAC provides an updated and searchable version of its SDN List at: https://sanctionssearch.ofac.treas.gov. OFAC requires all U.S. citizens to "block" (i.e., freeze) the assets of individuals and companies who are engaging in transactions with (i) countries that are subject to U.S. economic sanctions, (ii) certain companies and entities that act as agents for such countries, and (iii) certain individuals that act as agents for such countries. It is important to have a compliance program in place to avoid (or mitigate) receiving civil and criminal penalties from OFAC for non-compliance. See 31 C.F.R. Part 501 (OFAC Reporting Regulations); OFAC Economic Sanctions Enforcement Guidelines (November 9, 2009).

On February 13, 2018, in response to a letter from Senator Ron Wyden, an official within the Treasury issued a correspondence that called into question whether ICO issuers were *de facto* MSBs that were required to register with FinCEN. While there were several flaws in the logic set forth in the letter, it remains an area of concern for anyone considering a token sale. To add more confusion, speaking at a conference on November 19, 2019, FinCEN Director Kenneth Blanco, responding to a question about Facebook's plan to issue a cryptocurrency pegged to the U.S. dollar, stated that stablecoin issuers and dealers are money transmitters and must follow the BSA's AML laws.

State laws on money transmission vary widely but can generally be grouped into a few categories. Most states define money transmission as including some or all of three types of activities: (1) money transmission; (2) issuing and/or selling payment instruments; and (3) issuing and/or selling stored value. A few states only regulate these activities when "money" is involved, and define money as "a medium of exchange that is authorized or adopted by a domestic or foreign government." Generally, state money transmission laws apply to any entity that is either located in the state or is located outside of the state (including in a foreign jurisdiction) but does business with residents of the state. A novel solution to the redundancy of attaining state licenses is to become a New York limited purpose trust company. This may seem counterintuitive, as New York has the most onerous money transmitter licensing requirements for cryptocurrency companies, but this type of trust company charter exempts the company from many states' money transmission laws and requirements, while also providing the ability to conduct a broad range of custody and fiduciary services related to cryptoassets. Nevada and Wyoming have since followed New York and now permit the creation of special purpose depository institutions.

Another tension point for AML laws is the emergence of DeFi. DeFi is the permissionless decentralization version of various traditional financial instruments with a focus on exchanging assets, lending and borrowing and the creation of synthetic assets. For example, Uniswap is a decentralized exchange in the form of four smart contracts hosted on the Ethereum blockchain, as well as a public, open-source, front-end client. This ultimately allows for anyone with an internet connection to trade many Ethereum-native tokens with other users of the application. Inherent with its open-source nature, Uniswap does not have a customer identification vetting process and, in fact, circumventing AML laws is touted as one of Uniswap's foundational values among the cryptocurrency community. According to official data, over $620 billion of transactions occurred using the Uniswap Protocol in 2022. In September 2021, it was reported that the SEC had begun an investigation into Uniswap Labs and its Uniswap Protocol. This investigation is apparently ongoing.

In August 2022, OFAC sanctioned the popular cryptocurrency mixer Tornado Cash, adding it to the SDN List with 38 unique cryptocurrency addresses included as identifiers. Built on the Ethereum blockchain, Tornado Cash is the predominant example of a smart contract mixer. Tornado Cash is non-custodial. Users simply send the funds they want to mix to the Tornado Cash smart contract, and in return receive a cryptographic note they can use to withdraw their mixed funds to a new address by sending a transaction that references their note. OFAC specifically pointed to Tornado's role in laundering over $455 million worth of cryptocurrency stolen from Axie Infinity's Ronin Bridge Protocol by the North Korea-affiliated hacking organization, Lazarus Group. This designation suggests that decentralized protocols may be subject to some of the compliance obligations to which centralized services are held. Under Secretary of the Treasury for Terrorism and Financial Intelligence, Brian E. Nelson said the following in OFAC's press release on the Tornado Cash designation:

> Despite public assurances otherwise, Tornado Cash has repeatedly failed to impose effective controls designed to stop it from laundering funds for malicious cyber actors on a regular basis and without basic measures to address its risks. Treasury will continue to aggressively pursue actions against mixers that launder virtual currency for criminals and those who assist them.

Nelson's words make it clear that cryptocurrency services, whether they are decentralized or not, must at least make an effort to implement controls to prevent bad actors from abusing them.

In November 2022, OFAC settled with Kraken, a crypto exchange, for apparent violations of OFAC sanctions against Iran. According to the settlement letter, while Kraken maintained controls intended to prevent users from initially opening an account while in a sanctioned jurisdiction, it did not implement IP address blocking on transactional activity across its platform, allowing account holders who established their accounts outside of sanctioned jurisdictions to apparently access their accounts and transact on Kraken's platform from a sanctioned jurisdiction. Additionally, in 2023, OFAC issued an enforcement release announcing settlement of charges against virtual currency exchange Poloniex, under which Poloniex agreed to pay $7,591,630 for processing transactions totaling $15,335,349 between January 2014 and November 2019 in apparent violation of U.S. economic sanctions against Crimea, Cuba, Iran, Sudan, and Syria.

Taxation

In March 2014, the IRS declared that "virtual currency," such as Bitcoin and other cryptocurrency, will be taxed by the IRS as "property" and not currency. See IRS Notice 2014-21, Guidance on Virtual Currency (March 25, 2014). Consequently, every individual

or business that owns cryptocurrency will generally need to, among other things, (i) keep detailed records of cryptocurrency purchases and sales, (ii) pay taxes on any gains that may have been made upon the sale of cryptocurrency for cash, (iii) pay taxes on any gains that may have been made upon the purchase of a good or service with cryptocurrency, and (iv) pay taxes on the fair market value of any mined cryptocurrency, as of the date of receipt.

For an individual filing a federal income tax return, the gains or losses from a sale of virtual currency that was held as a "capital asset" (i.e., for investment purposes) are reported on (i) Schedule D of IRS Form 1040, and (ii) IRS Form 8949 (Sales and Other Dispositions of Capital Assets). Any realized gains on virtual currency held for more than one year as a capital asset by an individual are subject to capital gains tax rates. Any realized gains on virtual currency held for one year or less as a capital asset by an individual are subject to ordinary income tax rates. The IRS requires, on Form 8949, for each virtual currency transaction, the following information be disclosed: (i) a description of the amount and type of virtual currency sold; (ii) the date acquired; (iii) the date the virtual currency was sold; (iv) the amount of proceeds from the sale; (v) the cost (or other basis); and (vi) the amount of the gain or loss. It should be noted that the record-keeping requirements of IRS Form 8949 can be particularly onerous for those who have used cryptocurrency to make numerous small purchases of goods or services throughout the year.

For transactions completed on or after January 1, 2018, the Internal Revenue Code now prohibits the use of Section 1031(a) for cryptocurrency transactions, and requires a taxpayer to recognize taxable gain or loss at the time that any cryptocurrency is converted into another cryptocurrency. Section 13303 of P.L. 115-97 (the tax act signed into law on December 22, 2017) changes Section 1031(a) to state as follows: "No gain or loss shall be recognized on the exchange of real property held for productive use in a trade or business or for investment if such real property is exchanged solely for real property of like kind which is to be held either for productive use in a trade or business or for investment."

For transactions completed on or prior to December 31, 2017, the IRS has not issued any guidance on whether different cryptocurrencies are "property of like kind" that would qualify for non-recognition of gain under Section 1031(a). Generally speaking, exchanges between different cryptocurrencies are usually done by either (i) a simultaneous swap of one cryptocurrency for another, or (ii) a deferred exchange, in which one cryptocurrency is sold for cash, followed by the purchase for cash, of a different cryptocurrency.

For transactions completed on or prior to December 31, 2017, Section 1031(a)(1) of the Internal Revenue Code states the following: "No gain or loss shall be recognized on the exchange of property held for productive use in a trade or business or for investment if such property is exchanged solely for property of like kind which is to be held either for productive use in a trade or business or for investment." In 26 C.F.R. 1.1031(a)-2(b), "like kind" is defined as follows: "As used in section 1031(a), the words like kind have reference to the nature or character of the property and not to its grade or quality. One kind or class of property may not, under that section, be exchanged for property of a different kind or class." It should be noted that, in order to attempt to utilize the tax treatment of Section 1031(a) for transactions done on or prior to December 31, 2017, (i) each transaction must comply with certain requirements set forth in IRS regulations (such as the use, in certain instances, of a "qualified intermediary"), and (ii) the taxpayer must file a Form 8824 with the IRS.

There is a risk that the IRS could use its prior revenue rulings on gold bullion as a basis for taking the position that, for transactions completed on or prior to December 31, 2017, different cryptocurrencies are not "property of like kind" under Section 1031(a). In Rev.

Rul. 82-166 (October 4, 1982), the IRS ruled that an exchange of gold bullion for silver bullion does not qualify for non-recognition of gain under Section 1031(a). The IRS stated: "Although the metals have some similar qualities and uses, silver and gold are intrinsically different metals and primarily are used in different ways. Silver is essentially an industrial commodity. Gold is primarily utilized as an investment in itself. An investment in one of the metals is fundamentally different from an investment in the other metal. Therefore, the silver bullion and the gold bullion are not property of like kind." The IRS also stated in Rev. Rul. 79-143 (January 5, 1979) that an exchange of $20 U.S. gold numismatic-type coins and South African Krugerrand gold coins does not qualify for non-recognition of gain under Section 1031(a). The IRS stated: "The bullion-type coins, unlike the numismatic-type coins, represent an investment in gold on world markets rather than in the coins themselves. Therefore, the bullion-type coins and the numismatic-type coins are not property of like kind."

With respect to digital assets acquired via a hard fork or airdrop, the IRS issued Rev. Rul. 2019-24. Pursuant to this revenue ruling, the IRS confirmed that the new assets resulting from such events can result in revenue to the taxpayer. The IRS also concluded, however, that a taxpayer does not have gross income as a result of a hard fork if it does not receive the new cryptocurrency. In April 2021, the IRS released Chief Counsel Advice memo 202114020 (Hard Fork CCA) that specifically addressed the tax consequences of the 2017 hard fork that created Bitcoin Cash. The IRS concluded that a taxpayer who received Bitcoin Cash as a result of the hard fork had realized gross income. The IRS further concluded that when the taxpayer obtained "dominion and control" over the Bitcoin Cash would determine, for tax purposes, its date of receipt and the determination of its fair market value.

In November 2021, President Biden signed into law the Infrastructure Investment and Jobs Act ("**IIJA**"), which will require digital asset brokers to report to the IRS digital asset transactions valued at more than $10,000. IIJA defines the term "broker" broadly, which could subject parties that are peripheral to digital asset transactions, including cryptominers, software developers, and parties validating cryptocurrency transactions or selling cryptocurrency storage devices, to the reporting and compliance requirements of IIJA. In February 2022, the Treasury indicated that it is inclined to adopt a narrow interpretation of the term "broker" in the context of IIJA, which would limit compliance requirements for digital asset transactions to parties that can provide information useful to the IRS. These rules are scheduled to take effect in January 2024. In September 2022, Ethereum made the transition from a power-hungry, proof-of-work system ("**PoW**") to an environmentally friendly proof-of-stake system ("**PoS**") that uses over 99.9% less energy. This historic event was called "The Merge." The Merge changed the way that Ethereum transactions were validated. Using PoW, Ethereum worked like Bitcoin: transactions were mined by a decentralized network of computers, which raced to solve mathematical puzzles and were rewarded with new coins for doing so. Now, transactions are conducted on the new PoS network and new Ether will be minted by nodes on the network staking a fair amount of Ether tokens into a pool to secure the network and validate transactions.

For its part, the IRS has published guidance regarding the treatment of cryptocurrency staking rewards. In Rev. Rul. 2023-14, the IRS clarifies that when taxpayers stake cryptocurrency and receive validation rewards, the fair market value of the rewards must be included in the taxpayers' gross income for the taxable year when the taxpayer gains control over the rewards. A taxpayer has control over rewards once the taxpayer gains the ability to sell, exchange, or dispose of the received units.

Promotion and testing

Arizona became the first state in the U.S. to adopt a "regulatory sandbox" to shepherd the development of new emerging industries like fintech, blockchain and cryptocurrencies within its borders. The law grants regulatory relief for innovators in these sectors who desire to bring new products to market within the state. Under the program, companies are able to test their products for up to two years and serve as many as 10,000 customers before needing to apply for formal licensure. Other states have since followed suit and created similar programs including Wyoming, Florida, Utah, West Virginia, Kentucky, Vermont, Nevada and Hawaii.

Ownership and licensing requirements

Cryptocurrency fund managers that invest in cryptocurrency futures contracts, as opposed to "spot transactions" in cryptocurrencies, are required to register as a commodity trading advisor ("**CTA**") and commodity pool operator ("**CPO**") with the CFTC and with the National Futures Association (the "**NFA**"), or satisfy an exemption. Also, because of additions to the Dodd-Frank Act, cryptocurrency hedge fund managers that use leverage or margin would also need to register with the CFTC and NFA. The Dodd-Frank Act amended the Commodities Act to add new authority over certain leveraged, margined, or financed retail commodity transactions. The CFTC exercised this jurisdiction in an action against BFXNA INC. d/b/a BITFINEX in 2016. Fund managers should be cautious when using margin/leverage as it may require them to register as a CTA and CPO with the CFTC and register with the NFA. In April 2022, FalconX, a prime broker for digital assets that provides institutional investors access to the over-the-counter crypto derivatives market, announced that it has become the first cryptocurrency swap dealer registered with the NFA.

Quashing an industry-wide perception that DeFi actors are immune to regulatory scrutiny, in 2023, a federal judge in the U.S. District Court of the Northern District of California ruled that a DAO violated the CEA. In a precedent-setting decision, the court held that the defendant, Ooki DAO, is a "person" under the CEA and can thus be held liable for violations of the law, engaging in unlawful off-exchange leveraged and margined retail commodity transactions, soliciting and accepting orders for leveraged or margined retail commodity transactions with customers, and accepting money or property to margin those transactions.

The CEA assigns liability to "[a]ny person" who takes particular actions and defines "person" to include "individuals, associations, partnerships, corporations, and trusts." However, the CEA does not further define "association." The court noted that it had previously found that the CFTC sufficiently pleaded facts showing that Ooki DAO is an unincorporated association. Although that holding was in the context of a service of process issue, the court said those definitions were not limited to service provision. Thus, for those same reasons, the CFTC's complaint established Ooki DAO as an unincorporated association under state and federal law.

The Investment Company Act of 1940 (the "**Company Act**"), the Investment Advisers Act of 1940 (the "**Advisers Act**"), as well as state investment advisor laws, impose regulations on investment funds that invest in securities. The Company Act generally requires investment companies to register with the SEC as mutual funds unless they meet an exemption. Cryptocurrency funds, and hedge funds generally, can be structured under one of two exemptions from registration under the Investment Company Act. Section 3(c)(1) allows a fund to have up to 100 investors. Alternatively, Section 3(c)(7) allows a fund to have an unlimited number of investors (but practically it should be limited to 2,000 to avoid being deemed a publicly traded partnership under the Securities Exchange Act) but requires

a significantly higher net worth suitability requirement for each investor (roughly $5 million for individuals, $25 million for entities). As a general rule, most startup funds are structured as 3(c)(1) funds because of the lower investor suitability requirements.

Until the SEC provides more guidance on classifying individual cryptocurrencies as securities or commodities, the likelihood of many cryptocurrencies being deemed securities is high. As such, we recommend that cryptocurrency funds that invest in anything other than Bitcoin, or Ether, and the handful of other clearly commodity coins, comply with the Company Act preemptively. For most startup funds, this would mean limiting investors within a given fund to fewer than 100 beneficial owners.

Regardless of whether a startup cryptocurrency fund manager is required to register as a CPO/CTA with the CFTC under the Commodities Act, or register or seek exemption from the SEC as an investment advisor (under the Advisers Act), or investment company (under the Company Act), every cryptocurrency fund manager will be subject to the fraud provisions of the CFTC and/or the SEC. In September 2017, the CFTC announced its first anti-fraud enforcement action involving Bitcoin. These anti-fraud actions can be taken by the SEC and CFTC regardless of the cryptocurrency fund's exempt status.

In July of 2020, the OCC affirmed in an interpretive letter that national banks and savings associations can provide custody services for cryptocurrency. The letter noted that banks can also provide related services such as cryptocurrency-fiat exchanges, transaction settlement, trade execution, valuation, tax services and reporting. The effort supplements a patchwork of state regulation and guidance that to date has encouraged only a select few national banks and financial services companies to embrace cryptocurrency (see above: *Money transmission laws and anti-money laundering requirements*). While the OCC agreed that underlying keys to a unit of cryptocurrency are essentially irreplaceable if lost, it said that banks could be a part of the solution by offering more secure storage services compared to existing options.

Mining

The development of cryptocurrency and other popular blockchain applications has captured the attention of energy and environmental policymakers, global economists, and renewables industry players. Now home to over a third of the global computing power dedicated to mining Bitcoin, the U.S. has turned its attention to domestic miners and their impacts on the environment and local economies. On January 20, 2022, the U.S. House of Representatives Committee on Energy and Commerce's Subcommittee on Oversight and Investigations held a hearing, where the externalities of cryptocurrency mining were the focus of the agenda. An early indicator of the Subcommittee's views on the issue, the title for the hearing was "Cleaning up Cryptocurrency: The Energy Impacts of Blockchains." As the federal government studies the viability of crypto mining at a national level, states have been active in regulating crypto mining. In June 2022, the New York State Senate passed Senate Bill S6486D, which would establish a two-year moratorium on cryptocurrency mining operations that use PoW authentication methods to validate blockchain transactions in the state of New York. If signed into law, the bill would require comprehensive generic environmental impact review and effectively suspend all blockchain mining operations running on carbon-based power sources. Conversely, the Oklahoma Senate introduced Bill 590, which would establish the Commercial Digital Asset Mining Act of 2022 to provide certain tax exemptions for the sale of certain crypto mining equipment and machinery. Kentucky also enacted certain state-tax exemptions for cryptocurrency miners and mining facilities.

Border restrictions and declaration

A group of U.S. lawmakers has proposed a requirement that individuals declare their cryptocurrency holdings when entering the U.S., but to date no such requirement has gone into effect.

Reporting requirements

On December 31, 2020, FinCEN issued a notice stating that it intends to amend regulations implementing the BSA to include virtual currencies as a type of reportable account for the requirement to file a Report of Foreign Bank and Financial Accounts.

Estate planning and testamentary succession

Cryptocurrency, such as Bitcoin, has value and therefore is increasingly likely to become an estate asset. While there are few, if any, laws specific to cryptocurrency, due to the nature of cryptocurrencies, typical wills and revocable living trusts may not be well suited to efficiently transfer this new type of asset. Consequently, new estate planning questions and clauses may be needed.

While cryptocurrency is not sufficiently mature to allow existing legal structures to promulgate a complete set of rules and regulations, cryptocurrency's technological character allows estate planning to protect the intent of clients holding cryptocurrency. However, the lack of statutory structure necessitates proactive steps. Accordingly, someone who wants greater certainty of bequeathing cryptocurrency to their heirs will need to provide specific and detailed written instructions in your estate planning documents. The information they will need to include will depend upon the type of virtual currency wallet they have.

There are a wide range of cryptocurrency wallets that are available at this time. The current types of cryptocurrency wallets include: (i) a single device software wallet in which you hold the private keys (example: BitPay Wallet), (ii) a multiple device web wallet in which you hold the private keys (example: Blockchain Wallet), (iii) a multiple device web wallet in which you do not hold the private keys (example: Coinbase Wallet), (iv) a USB hardware dongle wallet in which you hold the private keys (example: Trezor Wallet), and (v) a "paper wallet" in which the private keys and public keys are written down (which can be later loaded into a software wallet of your choice to be spent).

The instructions that you provide in a will (for your personal representative) or in a declaration of trust (for the successor trustee of a revocable living trust) should be written in a manner that is easy to understand for individuals who are not familiar with cryptocurrency. For example, in the case of a single device software wallet in which you hold the private keys, instructions could include (i) a description of the name and version of the wallet software, (ii) a description of the name and version of the operating software system of the wallet device (i.e., iOS, Android, macOS, Windows or Linux), (iii) a description of the types of virtual currency held by the wallet, (iv) either the long-form private and public keys for the wallet or the 12-word "seed" BIP39 or BIP44 recovery phrase for the wallet, and (v) step-by-step instructions (which may include screenshots) showing how the wallet can be restored onto a new device, if the current wallet device cannot be accessed.

As transfers from a Bitcoin wallet and most other wallets are irrevocable, private key information about your cryptocurrency accounts will need to be kept in a secure manner. Security can be enhanced by storing the private key information in a safe-deposit box or vault, which could only be accessed after your death by the personal representative designated in your will (or the successor trustee designated in your revocable living trust).

Josias N. Dewey
Tel: +1 305 374 8500 / Email: joe.dewey@hklaw.com

Josias "Joe" N. Dewey is a finance and real estate attorney with the law firm of Holland & Knight LLP. Mr. Dewey also serves as the firm's Innovation Partner and is a member of the firm's Practice and Operations Committee. In addition, Mr. Dewey co-chairs the firm's Technology and Telecommunication Industry Sector Group. Mr. Dewey regularly represents a diverse group of banks and other financial institutions, from large international banks to local community banks. In addition to his traditional finance practice, a significant portion of Mr. Dewey's practice involves blockchain technology. Mr. Dewey has served in various court-appointed capacities in connection with enforcement actions brought by the U.S. Securities and Exchange Commission, including federal receiver, independent intermediary and Fair Fund distribution agent. Some of these engagements have involved extensive asset recovery efforts where the principal assets were digital assets, such as Bitcoin and Ether. Mr. Dewey is the co-author of the book, "*The Blockchain: A Guide for Legal and Business Professionals*."

Samir Patel
Tel: +1 305 789 7629 / Email: samir.patel@hklaw.com

Samir Patel is an innovation and technology attorney in Holland & Knight's Miami office and head of the firm's Document Automation Program. Mr. Patel works with financial institutions, insurance companies and corporate legal departments on implementing intelligent process automation within financial transaction and litigation workflows. Also, with a technical background in blockchain technology and smart contracts, Mr. Patel represents startups and emerging growth companies navigating the legal and regulatory issues encountering the nascent industry. Additionally, Mr. Patel works with artists, art galleries and athletes looking to enhance their products and brands through the creation of non-fungible tokens (NFTs), and advises on their market entrance strategy into the metaverse.

Holland & Knight LLP

701 Brickell Avenue, Suite 3300, Miami, FL 33131, USA
Tel: +1 305 374 8500 / Fax: +1 305 789 7799 / URL: www.hklaw.com

www.globallegalinsights.com

Global Legal Insights – Blockchain & Cryptocurrency Regulation provides in-depth analysis of blockchain and cryptocurrency laws and regulations across 33 jurisdictions, discussing government attitudes and definitions, cryptocurrency regulation, sales regulation, taxation, money transmission laws and anti-money laundering requirements, promotion and testing, ownership and licensing requirements, and mining.

Also in this year's edition are 13 Expert Analysis chapters, including in-depth guidance and analysis on cryptocurrency compliance, stablecoin regulation, digital asset sanctions, KYC/AML perspectives, cryptocurrency insolvencies, and taxation. Also covered in this year's edition are blockchain decentralisation, intellectual property, and NFTs, making this the definitive legal guide to the global blockchain and cryptocurrency industry in 2024.

GLI GLOBAL LEGAL INSIGHTS