GLI GLOBAL LEGAL INSIGHTS

Blockchain & Cryptocurrency Regulation

2022

Fourth Edition

Contributing Editor: **Josias N. Dewey**

glg global legal group

BLOCKCHAIN ALLIANCE · ENTERPRISE ETHEREUM ALLIANCE · Value Technology Foundation · WSBA WALL STREET BLOCKCHAIN ALLIANCE

Global Legal Insights
Blockchain & Cryptocurrency Regulation

2022, Fourth Edition
Contributing Editor: Josias N. Dewey
Published by Global Legal Group

GLOBAL LEGAL INSIGHTS – BLOCKCHAIN & CRYPTOCURRENCY REGULATION

2022, FOURTH EDITION

Contributing Editor
Josias N. Dewey, Holland & Knight LLP

Publisher
James Strode

Production Editor
Megan Hylton

Senior Editor
Sam Friend

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 978-1-83918-151-1
ISSN 2631-2999

Printed and bound by TJ Books Limited, Trecerus Industrial Estate, Padstow, Cornwall, PL28 8RW
October 2021

CONTENTS

PREFACE

It should come as no surprise that regulatory clarity in the digital assets (or crypto) space has remained elusive over the last 12 months. Nevertheless, interest in regulating digital assets and crypto has never been higher among policymakers and regulators. In the U.S., 2021 also ushered in a new administration. While it is still early days, some U.S. regulators already appear to be approaching digital assets from a different perspective (e.g., the Office of the Comptroller of the Currency). Others, however, appear to be doubling down on their historic approach (e.g., the Securities and Exchange Commission). All of this ensures that providing sound legal counsel in this space will continue to be a challenge. Now in its fourth edition, this publication is dedicated to assisting counsel overcome this challenge, whether advising clients in the U.S. or elsewhere.

The last year has seen a number of developing trends. First, the interest of institutional players has continued to grow exponentially as digital assets continue to move into the mainstream. This has included institutional investors and asset managers and the growing number of service providers and professionals that support those activities. Today, it is a rare event that an hour passes in which any financial news ticker does not include headlines about Bitcoin or other digital assets. Second, the proliferation of stablecoins and increasingly complex and popular decentralized finance transactions has drawn increased scrutiny from regulators and policymakers, with even the White House recently announcing that it supports regulating stablecoin issuers like banks. Third, non-fungible tokens (NFTs) have increased in popularity. NFTs representing everything from digital artwork to sports memorabilia fetched millions at auction. Simply put, the number and nature of engagements has exploded over the last year.

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, privacy coins, such as Monero, potentially allow for digital transfers of value without an easy means of identifying senders and recipients. This has implications for the application of AML/KYC regulations, such as the travel rule, to transactions involving these assets. 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

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 fourth edition publication of *GLI – Blockchain & Cryptocurrency Regulation*. As usual, GLG has assembled a remarkable group of leaders in the legal industry to analyze and explain this complex yet exciting environment.

What a difference a year makes! From DeFi to NFTs, from decentralized exchanges to bridges, from digital assets to CBDCs, we are witnessing first-hand a revolution in how trust and agreements are managed, for any and all transactions between two or more parties. With financial assets and transactions tied to blockchain racing towards USD 1 trillion, the adoption rate of the technology surpassing that of the early Internet, and countries rolling out digital versions of their currencies, this wave is no longer coming; it's here. The rapidity with which the technology is entering commerce has been a wake-up call to regulatory and legislative bodies the world over, with legal, financial, and accounting firms scrambling to keep up. It is within this context that we thank each of the authors who have so graciously contributed their expertise to this volume. We hope, and expect, that readers will find this publication useful as they navigate this rapidly rising wave.

The EEA is the industry's first member-driven global standards organization, known for developing open blockchain specifications that drive harmonization and interoperability for businesses and consumers worldwide. The EEA's world-class Enterprise Ethereum Client Specification, Off-Chain Trusted Compute Specification, and forthcoming EthTrust and Authority to Operate specifications, will ensure 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

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.

The evolution of global markets continues – Blockchain, cryptoassets and the future of everything

Ron Quaranta
Wall Street Blockchain Alliance

This 2022 edition of the "*GLI – Blockchain & Cryptocurrency Regulation*" publication comes at a time when the world continues to reel from the effects of the COVID-19 pandemic, as well as the subsequent economic downturn caused in large part by business shutdowns around the globe. That said, in these challenging times it is fascinating to see the ongoing evolution of both blockchain technology and cryptoassets across a wide variety of industries. In fact, many enterprises have begun to expand their efforts to advance the use of blockchain technology in different markets, for different clients and for a myriad of different use cases. And the Wall Street Blockchain Alliance, with members encompassing some of the largest banks, brokerages, institutional investors, legal practices, and technology firms in the world, is proud to stand alongside these members and other partners at the forefront of this evolution.

At this point in time, readers of the latest edition are probably no longer just familiar with the proposed benefits of blockchain technology such as decentralization, immutability, auditability, and transparency, but are just as likely to be involved in proof of concepts or pilot projects related to their firms' engagement with this technology, either directly or in firm engagements with partners, vendors, clients, regulators and more. Indeed, in keeping with the theme of this book, it is important to keep in mind that the regulatory landscape continues to evolve in the wake of the innovations to be discussed in this chapter. Likewise, it is important for readers to keep abreast of these regulations, to be aware of the regulatory perspectives on blockchain technology and cryptoassets and ultimately to be prepared to engage the ecosystem in a way that is compliant as well as adds true value and return on investment around the world.

The world of global finance and banking, which many would argue is the reason that blockchain and cryptoassets were invented in the first place, are transforming in ways that many would not have considered possible in the past several years. In many respects, blockchain and cryptoassets are fundamentally reshaping how people invest, borrow, and save and have initiated what many see as a parallel universe of alternative financial services, allowing cryptoassets to begin to move into traditional banking territory.

For example, firms such as BlockFi[1] and Nexo,[2] as well as major crypto exchanges such as Coinbase[3] and Gemini,[4] allow users to earn "interest" on balances of Bitcoin, Ethereum and other cryptoassets, often at rates notably higher than in current banking offerings. Alternatively, clients can also borrow with crypto as collateral to back a loan, with in some instances these crypto loans involving no credit checks since transactions are backed by cryptoassets. To be clear, these nascent banking-like capabilities are still a bit more exotic than most are familiar with, and regulators unsurprisingly have cast a critical eye on these offerings, and come with their own series of risks, including lack of deposit insurance and minimal, if any, reserves. Indeed, as of this writing, several state regulators in the United States have ordered firms to cease these offerings in their respective jurisdictions.[5]

This should not suggest, however, that firms are operating in a wholesale "illicit" manner. Notably, many of the more prominent of these firms have applied for and received the necessary state lender licenses and, in some instances, bank charters, including Kraken Bank, which was granted a Wyoming bank charter and is planning to soon accept retail deposits. All this activity, while representing what many see as the evolution of global financial markets, continues to invoke concern from regulators and legislators. This is particularly true as these businesses grow in size. The aforementioned BlockFi, now firmly in the sights of Washington, D.C., claims to have over US$10 billion in assets.[6] Similar focus is occurring in Germany, Singapore and other nations, though there is a perspective in the cryptoassets industry that nations outside of the United States are more innovative and possibly accepting of cryptoasset usage. Only time, of course, will tell.

Stablecoins, noted in the previous edition, continue their upward march towards global industry usage, if not necessarily widespread acceptance, with a global market cap of over US$100 billion as of this writing. These tokens, which are meant to minimize the associated volatility of cryptoassets by having them backed by or "pegged" to an underlying asset such as the U.S. dollar, or other currencies or commodities, continue to garner interest by enterprises and investors, as well as regulators around the world. However, there continue to be challenges in their usage, including reporting, taxation, valuation and more. In addition, the stablecoin arena continues with some level of controversy. One need only read those latest challenges associated with the stablecoin Tether,[7] and whether the token is truly backed by the U.S. dollar, to understand some of the ongoing concerns in this arena.

One of the most notable developments in the past year has been the very rapid rise of decentralized finance, or "DeFi," in the cryptoasset arena. In the prior edition, the value of all DeFi offerings stood at approximately US$4 billion. That number is now well over US$150 billion[8] and climbing. Previously known as "open finance," DeFi is designed to provide many of the same capabilities available in global financial markets currently, with one very significant difference; that is, the ability to fully engage with the digital assets in a fully decentralized, open system, with no central party or intermediary (such as banks or brokerage firms). Giving participants in a DeFi marketplace full control over their assets offers the potential for a seismic shift in how global markets operate and offer the potential for a wide variety of benefits and new financial models. And by some accounts, DeFi will possibly allow for greater participation by the unbanked and underbanked in global financial markets. However, DeFi is not without its challenges and risks. Some of the more prominent risks include poor smart contract creation and auditing, user error, market volatility, and much more. Despite its size, DeFi is still a nascent market. While it will continue to draw risk investment, much work still needs to occur to allow for its widescale acceptance. One final note on DeFi that is worth consideration is that DeFi, in many viewpoints, represents a fundamental shift in how individuals and businesses can participate in global banking and financial markets. This shift strikes at the heart of why some intermediaries such as banks and brokerage firms exist, and it is not surprising that these businesses, as well as the regulators and legislators focused on them, take a poor (if fundamentally misunderstood) view of DeFi. Readers can probably expect further regulatory concern and action on DeFi in the coming months and years, but as is often noted in the industry, you cannot undo the innovation. How much DeFi disrupts global markets is still to be determined, but it is sure to be an interesting ride.

Central Bank Digital Currencies, or "CBDCs," have also risen in prominence in the past year. At its core, the concept of CBDC is a type of "currency" that governments around the world are considering and which is based upon blockchain technology, with the goal of lowering

costs and increasing the overall efficiency and effectiveness of their payments systems. Given the friction associated with existing payments systems, including time delays and costs, the benefits to proponents of a CBDC are clear. That said, CBDCs are very much in the earliest stages, with the more developed proposals being the Chinese digital yuan, which is currently in a pilot program, and has raised concerns with other nations around the world, including the United States, which are concerned that the Chinese CBDC may pose a threat to the U.S. dollar's reserve status.[9] At a technology level, critics claim that CBDCs do not represent the true promise of blockchain or distributed ledger technology in that governments would still play a central role in CBDC creation and management, hence negating the decentralized nature of blockchain and cryptoassets. Governments and central banks tend not to move rapidly towards new innovation, and readers should be confident that this innovation will take time and will be a topic of conversation for some time to come.

Finally, one cannot review the prior year of developments in the world of blockchain and cryptoassets without discussing Non-Fungible Tokens, or "NFTs." An NFT is essentially a digital asset (generally coded like cryptoassets) that represents either a digital or real-world object such as art or music. NFTs can be bought and sold online, normally with cryptocurrency. The NFT is, at its core, a data unit stored on a blockchain, which verifies the digital asset as unique and non-interchangeable. One of the most prominent examples of an NFT was the sale of an original piece of digital art by the artist known as "Beeple," who sold his "Everydays: the First 5000 Days" digital art for US$69 million in March of 2021 through Christie's Auction House.[10] Since then, there has been concern about an NFT "bubble" in prices, and indeed overall global prices have dropped in the NFT market. That said, NFT sales exceeded US$2.5 billion in the first half of 2021,[11] and the market continues to see new NFTs for everything from art to baseball cards to famous artist music and more. While proponents say that NFTs solve the problem of double spending of a digital asset as well as the benefit of digital scarcity, critics cite the environmental toll of NFTs (as they do with Bitcoin, for example), plagiarism concerns, and the overarching concerns about viable smart contract code and cybersecurity. However, the overall industry perspective is that as NFTs grow in usage, these concerns will be mitigated, and what will develop is a vibrant and stable way to exchange real and digital assets in a compliant and cost-effective way that imbues the holder with direct ownership rights embedded as part of the actual token itself. What might have seemed to be science fiction not too long ago, may become fact as even the real estate industry is looking to NFTs as a way for real property to change hands. While in comparison to the global financial system (or even the global cryptoasset market) NFTs are incredibly small in size, if the underlying industry discussions are any guide, they may become a multi-trillion-dollar market in the future.

To address the above issues and developments, the WSBA continues to operate 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. For example, working with members of the WSBA Legal Working Group, now totaling more than 180 attorneys and general counsels from more than 90 firms and practices globally, we were privileged to continue our work of open commentary and request for information responses with regulators and legislators around the world. These include the United States Securities and Exchange Commission, the Internal Revenue Service, the Office of the Comptroller of the Currency, the Federal Deposit Insurance Corporation and more. Internationally, we continue to dialogue and interact with the Financial Services Authority and will continue to do so in other regions of the world, particularly Asia and Africa.

Given the growing importance of blockchain and cryptoassets for global enterprises, it is not surprising that our Accounting Working Group, in cooperation with our accounting members as well as our partners at AICPA and CPA.com, has been notably busy. In addition to ongoing member meetings and practice workshops, the Accounting Working Group has published a series of critical whitepapers focused on Decentralized Finance and Non-Fungible Tokens, as well as an advanced Stablecoins publication, building on our primer from 2019.

Our Enterprise & Technology Working Group continues to serve as the path for partnerships with our members and global technology partners such as Hyperledger, the Linux Foundation, R3 and more. This Working Group has been the forum for our members to discuss, strategize and collaborate on deep technology solutions and prototypes, as well as learn about the latest innovations and offers from industry leaders from around the world. It is here that we also work through the ongoing challenges of blockchain technology and smart contract innovation, including cybersecurity, data privacy, integration, interoperability and more. These discussions highlight the need to comprehensively address these issues so that innovation can continue to grow and provide greater offerings in a safe and compliant manner.

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 the challenges and potential of cryptoassets, DeFi, and NFTs as they take their place in global portfolios.

Following on this, we recently launched our Tokenization Working Group, which will focus on the tokenization of both real and virtual assets, including art, wine, real estate and more. As the landscape of possible investable assets expands in ways we would never have imagined, understanding how these assets are created, valued, and traded in a safe and compliant way becomes ever more important. Our Tokenization Working Group exists to guide and promote this development for our global members across a multitude of industries.

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 an important reference for these fast-developing innovations. We look forward to an ongoing dialogue with our colleagues in all the different industries involved including law, banking, trading, supply chain and beyond.

* * *

Endnotes

1. https://blockfi.com/crypto-interest-account/.
2. https://nexo.io/.
3. https://www.coinbase.com/earn.
4. https://www.gemini.com/earn.
5. https://www.reuters.com/legal/transactional/new-jersey-orders-blockfi-cryptocurrency-firm-stop-offering-interest-bearing-2021-07-20/.
6. https://www.nytimes.com/2021/09/05/us/politics/cryptocurrency-banking-regulation.html.

7. https://www.theverge.com/22620464/tether-backing-cryptocurrency-stablecoin.
8. https://coinmarketcap.com/view/DeFi/.
9. https://www.cnbc.com/2021/07/24/the-us-is-deciding-how-to-respond-to-chinas-digital-yuan.html.
10. https://www.theverge.com/2021/3/11/22325054/beeple-christies-nft-sale-cost-everydays-69-million.
11. https://www.reuters.com/technology/nft-sales-volume-surges-25-bln-2021-first-half-2021-07-05/.

* * *

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 2021*", published 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 startups and corporations focused on fintech innovation and blockchain technology.

Wall Street Blockchain Alliance

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

Cryptocurrency and blockchain in the 117th Congress

Jason Brett & Whitney Kalmbach
Value Technology Foundation

The 117th United States Congress – in session from January 3, 2021 to January 3, 2023 – has so far arguably had the most activity with respect to cryptocurrency and blockchain technology in both the House of Representatives and the Senate. In May of 2021, three U.S. Senators – Senator Cynthia Lummis (R-WY), Senator Marsha Blackburn (R-TN), and Senator Kyrsten Sinema (D-AZ) – introduced the Financial Innovation Caucus, a bipartisan Caucus that will focus on a number of issues critical to the future of banking and ensure U.S. competitiveness on the global stage, including key concepts such as distributed ledger technology (blockchain), digital assets, and central bank digital currencies. In June of 2021, the Chairwoman of the House Committee on Financial Services, Congresswoman Maxine Waters (D-CA), introduced a Digital Assets Working Group of Democratic Members. According to the press release, the Digital Assets Working Group will focus on making sure there is responsible innovation in the cryptocurrency and digital asset space, where Members will work together on legislation and policy solutions regarding cryptocurrency regulation, the use of blockchain and distributed ledger technology, and the possible development of a Central Bank Digital Currency (CBDC).

Meanwhile, the President's Working Group on Financial Markets is preparing to release a report on stablecoins with recommendations on how to regulate the marketplace. For the first time, the Office of Foreign Assets Control (OFAC) has sanctioned a cryptocurrency exchange for its facilitation of a payment in a ransomware case. Much-publicised cases such as the Colonial Pipeline hack have brought attention to where cryptocurrency may be used in criminal activities. The Financial Action Task Force (FATF) provided a draft of updated rules around what is a Virtual Asset Service Provider (VASP) and added to its purpose the concept of Proliferator Finance (PF), where it already focuses on Money Laundering (ML) and Terrorist Financing (TF).

The industry continues to battle for regulatory clarity in the space, specifically with the newly appointed Chairman Gary Gensler of the Securities and Exchange Commission (SEC), who was formerly a Professor at the Massachusetts Institute of Technology (MIT) focusing on digital currencies and blockchain technology. Gensler previously served as Chair of the Commodity Futures Trading Commission (CFTC), where he expanded that agency's powers to regulate derivatives after the financial crisis of 2008–2009. Gensler has focused on the notion that of the 50–100 tokens that may be bought and sold on a cryptocurrency exchange, the odds are that at least one – if not more – are securities. Thus, a cryptocurrency exchange is at risk of allowing the trade of unregistered securities and Gensler has encouraged exchanges to come to the SEC and talk with him – and "get registered".

Congress continued its activity of issuing bills that attempt to either clarify the regulatory space for cryptocurrency and blockchain tokens, highlight and expand the use of blockchain

for other use cases within the U.S. Government, and explore the possibility of issuing a CBDC or digital dollar in the United States.

There have been 25 bills introduced so far in 2021 that this chapter will summarise. The bills are divided into three sections: (1) cryptocurrency; (2) blockchain; and (3) CBDC. Regarding cryptocurrency, bills are designed to improve the way cryptocurrencies are regulated with respect to taxes as well as how the financial services regulators view tokens as either currencies, commodities, or securities. There is also an ask to view how blockchain technology via its tokens may provide ways to enhance minorities in being able to participate in the broader capital markets.

The blockchain or distributed ledger technology bills focus on ways to promote the technology within the U.S. Government or broader use and how to coordinate the technology amongst the various agencies. The technology that underpins the cryptocurrencies that are often traded for value is viewed as providing other use cases, whether that includes tokenisation of assets or tracking items on a supply chain.

Finally, the new concept of CBDCs continues to be explored – in contrast to the rising use of stablecoins that has the attention of federal regulators. Whether it is a stablecoin, or privately a representation of a U.S. dollar, the transfer as well as purchase of the equivalent of U.S. dollars within the cryptocurrency industry could be a greater threat to the U.S. dollar and monetary policy than Bitcoin or Ethereum.

All three of these areas – the regulation of cryptocurrencies, the blockchain technology that offers possibilities of a distributed ledger for every sector of the economy and other use cases, and the consideration of whether the United States needs to print its own CBDC – are equally important. However, the one that has seen the most attention recently relates to the way cryptocurrencies should be regulated and whether legislation is even needed, or whether the regulators can promulgate effective rules to help ensure that the banking system stays safe and sound and that consumer protection is also considered.

The abovementioned bills introduced this year include the following:

Cryptocurrency

1. Consumer Safety Technology Act.[1]
2. Cryptocurrency Tax Clarity Act.[2]
3. Cryptocurrency Tax Reform Act.[3]
4. Digital Asset Market Structure and Investor Protection Act.[4]
5. Digital Taxonomy Act.[5]
6. Eliminate Barriers to Innovation Act of 2021.[6]
7. End Banking for Human Traffickers Act of 2021.[7]
8. Financial Technology Protection Act.[8]
9. Infrastructure Investment and Jobs Act.[9]
10. RESCUE Act for Black and Community Banks.[10]
11. Safe Harbor for Taxpayers with Forked Assets Act of 2021.[11]
12. Sanction and Stop Ransomware Act.[12]
13. Securities Clarity Act.[13]
14. Token Taxonomy Act.[14]
15. Virtual Currencies and Global Competitiveness Act.[15]
16. U.S. Virtual Currency Market and Regulatory Competitiveness Act of 2021.[16]
17. U.S. Virtual Currency Consumer Protection Act of 2021.[17]

Blockchain legislation

1. Blockchain Innovation Act.[18]
2. Blockchain Promotion Act of 2021.[19]

3. Blockchain Regulatory Certainty Act.[20]
4. Blockchain Technology Coordination Act of 2021.[21]

Central bank digital currency legislation

1. 21st Century Dollar Act.[22]
2. Automatic BOOST to Communities Act.[23]
3. Central Bank Digital Currency Study Act of 2021.[24]
4. Communist China's Digital Currency – National Security Risks Act: national security implications of the People's Republic of China's efforts to create an official digital currency.[25]

Consumer protection: Digital tokens and blockchain technology

Two bipartisan blockchain bills originally introduced by Rep. Darren Soto (D-FL) passed the House of Representatives in the form of the Consumer Safety Technology Act (H.R. 3639), the Blockchain Innovation Act, and parts of the Digital Taxonomy Act (H.R. 3638). The Digital Taxonomy Act passed the House of Representatives as part of Rep. Jerry McNerney's (D-CA) bill, the Consumer Safety Technology Act (H.R. 3723). The bills also passed during the 116th Congress and were the first blockchain bills to pass the House. The Blockchain Innovation Act, co-sponsored by Rep. Brett Guthrie (R-KY), directs the Department of Commerce in consultation with the Federal Trade Commission (FTC) to conduct a study and submit to Congress a report on the state of blockchain technology and commerce, including its use to reduce fraud and increase security.

The Digital Taxonomy Act, co-sponsored by Rep. Warren Davidson (R-OH-08), requires the FTC to submit to Congress a report and recommendations on unfair deceptive trade practices in digital tokens.

The passage of the Consumer Safety Technology Act, its first section on artificial intelligence, and the inclusion of Rep. Soto's bills, represent a collaboration between the leaders of the Congressional Artificial Intelligence Caucus and the Congressional Blockchain Caucus, respectively.

Tax clarity

The Infrastructure Investment and Jobs Act (H.R. 3684) included two sections relating to cryptocurrency taxation reporting, i.e., new policy and part of a "pay-for" to ensure that the bill would not incur a deficit. Section 80603, Information Reporting for Brokers and Digital Assets, recommends changing the definition of who is a broker according to the Internal Revenue Service (IRS) from "any other person who (for consideration)" to "any person who (for consideration) is responsible for regularly providing any service effectuating transfers of digital assets on behalf of another person". The term "digital asset" is 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". Section 6050I(d) adds in to this section as including digital assets for treatment of cash, and that anyone who is engaged in a trade or business and receives more than $10,000 in digital assets is responsible to file a form that includes the name, address, and Taxpayer Identification Number of the person from whom the cash was received, the amount of cash received, the date and nature of the transaction, and such other information as the Secretary may prescribe.

In the case of section 80603, there was a great deal of discussion and an amendment that was attempting to exempt blockchain validators and software and hardware producers of the technology, as with these types of processes it is not possible to collect the information

required for reporting. Although an amendment was agreed upon on a bipartisan basis, the language was not included in the bill due to a procedural motion. The bill will soon be voted on in the House.

Both the Cryptocurrency Tax Clarity Act (H.R. 5082) and the Cryptocurrency Tax Reform Act (H.R. 5083) looked to find a way to provide a compromise on the way to exclude some of these processes by Rep. Soto.

The Token Taxonomy Act (H.R. 1628) included a provision that would adjust taxation of virtual currencies held in individual retirement accounts, to create a tax exemption for exchanges of one virtual currency for another, and would create a *de minimis* exemption from taxation for gains realised from the sale or exchange of virtual currency for an asset other than cash in the amount of $600 or less.

The Safe Harbor for Taxpayers with Forked Assets Act attempts to fix a problem where, in 2014, the IRS issued guidance that would treat digital assets like property. However, this bill attempts to provide a temporary safe harbour for many important questions that the IRS has not addressed, including when it comes to "forked" digital assets. A "fork" is one of the ways digital assets are different from a dollar bill in your wallet. A virtual currency exists on a blockchain, which creates a ledger of that currency's transaction history. If someone wants to use the open-source code of that existing blockchain to create a new blockchain, this will result in a fork: two blockchains and their respective virtual currencies. This means that a user who purchased one type of virtual currency could suddenly have that currency in their digital wallet along with a new currency, if the original blockchain was forked. For example, Bitcoin Cash is a fork of Bitcoin. A developer might create a fork to resolve a dispute between users or to address a security concern. The Safe Harbor for Taxpayers with Forked Assets Act will hold accountable harmless taxpayers attempting to report gains or losses of their forked digital assets. The bill also delineates that receipt of a forked virtual currency may not constitute a taxable event.

The grace period established under the bill will continue until the IRS sets a clear and consistent set of rules regarding the tax treatment of forked cryptocurrencies. The bill effectively prohibits penalties against taxpayers until the IRS issues updated guidance on how to report gains and losses in "forked" digital assets.

Congressman Tom Emmer (R-MN) submitted the same bill for the first time in 2018. In April of 2019, Congressman Emmer led a letter along with 20 Members of Congress to the IRS urging additional guidance. In October of 2019, the IRS issued guidance stating that the receipt of a forked virtual currency is a taxable event. Taxpayers who receive forked virtual currency, however, receive it automatically when the fork occurs, often unwillingly and unknowingly. The result is a tax policy that places an additional tax burden on taxpayers who have not realised any change, and in fact may have no knowledge of this new tax burden.

Enforcing sanctions, stopping use of cryptocurrencies for illegal trafficking and enhancing protection from financial technology that spurs money laundering or terrorist financing

U.S. Senators Marco Rubio (R-FL) and Dianne Feinstein (D-CA) introduced the Sanction and Stop Ransomware Act (S. 2666), a piece of legislation to strengthen the cybersecurity of critical infrastructure and target foreign governments that knowingly provide safe haven for cyber criminals. Among other important considerations, the bill would require the development of regulations for cryptocurrency exchanges operating to reduce anonymity of accounts and users suspected of ransomware activity and make records available to the U.S. Government in connection with ransomware incidents.

Rep. Ted Budd (R-NC) introduced the Financial Technology Protection Act (H.R. 296), which helps stop the illicit use of new financial technologies. The bill has twice passed the House unanimously in 2018 and 2019. The purpose of the bill is to fight crime using financial technology. This bill provides for the investigation of new financial technologies (e.g., digital currencies) and their use in terrorism and other illicit activities. Specifically, the bill establishes the Independent Financial Technology Task Force to Combat Terrorism and Illicit Financing, which must research terrorist and illicit use of new financial technologies and issue an annual report. The Department of the Treasury must establish a fund to provide a reward for a person who provides information leading to the conviction of an individual involved with terrorist use of digital currencies. Additionally, the bill establishes the FinTech Leadership in Innovation and Financial Intelligence Program to support the development of tools and programmes to detect terrorist and illicit use of digital currencies.

The End Banking for Human Traffickers Act of 2021 (H.R. 808) more broadly seeks to increase the role of the financial industry in combatting human trafficking, and specifically recommended changes, if necessary, to existing statutory law to more effectively detect and deter money laundering relating to severe forms of trafficking in persons, where such money laundering involves the use of emerging technologies and virtual currencies.

Cryptocurrency clarity for digital assets *vs* digital asset securities and the classification of digital assets as currencies, securities, and commodities

A bill was introduced called the Eliminate Barriers to Innovation Act of 2021, which will require the SEC and CFTC to establish a digital asset working group to ensure collaboration between regulators and the private sector to foster innovation. The Eliminate Barriers to Innovation Act will require the SEC and CFTC to establish a working group on digital assets that would be known as the SEC-CFTC Working Group on Digital Assets, which will consist of appointees from the Commission as well as representatives from financial technology companies, financial firms, and small businesses, among others. The working group will produce a report within a year that will include an analysis of the domestic regulatory framework and the developments in other countries relating to digital assets. The report also requests insight into best practices to reduce fraud, protect investors, and assist in compliance with obligations under the Bank Secrecy Act (BSA).

Other bills that have been introduced include the Securities Clarity Act. Congressman Tom Emmer (MN-06) introduced the bipartisan Securities Clarity Act with Reps Darren Soto (D-FL) and Ro Khanna (D-CA) to provide a clear definition of assets like digital tokens and other emerging technologies under current securities laws. The measure utilises a technology-neutral approach to remain adaptable to future innovations. Congressman Emmer's legislation provides a solution for individuals who have complied with existing securities registration requirements, or who have qualified for an exemption but, after meeting these requirements, innovative entrepreneurs may distribute their asset to the public without fear of additional regulatory burdens. These assets are in fact, and always were, commodities.

The legislation solidifies the status of any asset sold as the object of an "investment contract", a term with more than 75 years of jurisprudence, by proposing a new definition: "investment contract asset." The Securities Clarity Act states that an investment contract asset (for example, a digital token) is separate and distinct from the securities offering of which it may have been part. The approach is technology-neutral, and applies equally to all assets offered and sold, whether tangible or digital. This new defined term would refer

to any asset sold as part of an investment contract that would not be considered a "security" but for its sale as part of an investment contract.

Another bill that champions and seeks clarity among digital assets as to whether they are securities or commodities is the Token Taxonomy Act. Rep. Warren Davidson (R-OH) reintroduced what is his signature Token Taxonomy Act, which establishes much looked-for clarity for businesses, consumers, and regulators operating in the growing U.S. blockchain ecosystem, based on the notion that a patchwork of laws and regulations creates confusion and even hostility to various blockchain businesses, and that without a workable federal regulatory structure, many businesses and entrepreneurs are taking their businesses overseas where clearer and friendlier laws have established thriving blockchain economies. Market interest in cryptocurrencies and blockchain technology has continued to grow as certain cryptocurrencies have enjoyed a boom throughout the coronavirus pandemic and as the Biden Administration considers whether or not to continue regulation on private digital wallets started by the Trump Administration. Davidson commented that by establishing the appropriate regulatory environment, opportunities and advancements that blockchain innovation promises can happen here in the United States, for the benefit of Americans.

Congressman Darren Soto (D-FL) introduced two bipartisan bills, the Virtual Currency Consumer Protection Act of 2021 and the U.S. Virtual Currency Market and Regulatory Competitiveness Act of 2021, to help prevent virtual currency price manipulation and position the United States to be a leader in the cryptocurrency industry. The Virtual Currency Market and Regulatory Competitiveness Act of 2021, co-sponsored by Rep. Tom Emmer (R-MN), directs the CFTC to describe how price manipulation could happen in virtual markets and makes recommendations for regulatory changes to improve the CFTC's price manipulation prevention procedures.

Both bills are also co-sponsored by Reps Ted Budd (R-NC), Ro Khanna (D-CA), and Warren Davidson (R-OH). They direct the CFTC and other financial regulators to make critical recommendations to improve the regulatory environment for both the consumer and business development sides. These pieces of legislation are crucial in light of concerns raised in the New York Attorney General's recent report on virtual exchanges' risk of manipulation and the *Wall Street Journal*'s description of potentially abusive software of bots manipulating the price of Bitcoin.

These bills have been introduced in the past two Congressional sessions and have had success through the appropriations process as well. First, funding increases of $3 million to LabCFTC were included in the final FY20 appropriations package and signed into law. Additionally, report language based on portions of these bills was also included in the final FY20 appropriations package and resulted in a subsequent report by the CFTC. The language directs the Commission to prepare a report on how to better protect virtual currency investors and promote U.S. competitiveness in the realm of cryptocurrency.

The Digital Asset Market Structure and Investor Protection Act was introduced by Congressman Don Beyer (D-VA). Beyer notes that since the introduction of Bitcoin in late 2008, digital assets have evolved from technological curiosities into financial instruments used by millions of ordinary Americans. With over 11,000 separate digital asset tokens in existence, and a market capitalisation of over $1.5 trillion, an estimated 20–46 million Americans own Bitcoin and other digital assets, with that number only expected to grow. Beyer points out that many of these digital asset market participants, who are primarily average Americans rather than large institutional investors, have been victims of theft during trading platform hacks, or have been exposed to significant market manipulation or frauds such as Ponzi schemes.

Digital assets have also been widely used for money laundering and other illicit purposes. For instance, in May 2021, the Colonial Pipeline, which provides gasoline to much of the eastern United States, had its computer system hacked and was forced to pay a $4.4 million ransom in Bitcoin, which is the preferred currency for ransomware attacks. Despite the rapidly growing importance of Bitcoin and other digital assets in our economy, no comprehensive legal framework exists to regulate the digital asset market or protect market participants.

The Digital Asset Market Structure and Investor Protection Act of 2021 seeks to promote innovation and U.S. jobs by providing legal and regulatory certainty for digital assets, provide fundamental investor protections to U.S. retail investors and other consumers, improve trade reporting and transparency, strengthen the BSA requirements related to the treatment of digital assets, and protect U.S. investors in the digital asset sector. Specifically, the bill would create statutory definitions for digital assets and digital asset securities and provide the SEC with authority over digital asset securities and the CFTC with authority over digital assets. The bill would also provide legal certainty as to the regulatory status for the top 90 per cent of the digital asset market (by market capitalisation and trading volume) through a joint SEC/CFTC rulemaking. The bill would require digital asset transactions that are not recorded on the publicly distributed ledger to be reported to a registered "Digital Asset Trade Repository" within 24 hours to minimise the potential for fraud and to promote transparency. The bill would explicitly add digital assets and digital asset securities to the statutory definition of "monetary instruments", under the BSA, formalising the regulatory requirements for digital assets and digital asset securities to comply with anti-money laundering (AML), recordkeeping, and reporting requirements. The bill would provide the Federal Reserve with explicit authority to issue a digital version of the U.S. dollar, clarify that digital assets, digital asset securities and fiat-based stablecoins are not U.S. legal tender, and provide the U.S. Treasury Secretary with authority to permit or prohibit U.S. dollar- and other fiat-based stablecoins. The bill would direct the Federal Deposit Insurance Corporation (FDIC), National Credit Union Administration (NCUA), and Securities Investor Protection Corporation (SIPC) to issue consumer advisories on "non-coverage" of digital assets or digital asset securities to ensure that consumers are aware that they are not insured or protected in the same way as bank deposits or securities. Finally, the bill would require legislative recommendations from the Financial Crimes Enforcement Network (FinCEN), SEC and CFTC to provide clarity on dividing lines between who must register as a money services business *versus* who must register as a securities or commodities exchange.

Market competitiveness and supply chain challenges of mining cryptocurrency

U.S. Senators Maggie Hassan (D-NH), a member of the Homeland Security and Governmental Affairs Committee, and Joni Ernst (R-IA) have introduced bipartisan legislation to help improve oversight of cryptocurrency mining operations in foreign countries. The bill requires the Department of the Treasury to report to Congress on virtual currencies and their use globally – including how other countries are using and mining cryptocurrencies, and how cryptocurrency mining operations are impacting supply chains, including for critical technologies like semiconductors. Senator Hassan has also called on multiple federal agencies, including the Department of the Treasury, to address current aspects of the cryptocurrency market that allow for criminal usage, such as cyberattacks. Following Senator Hassan's calls, the Department of the Treasury announced a number of actions to crack down on the use of cryptocurrency for receiving ransomware payments and conducting other illegal activities.

The Senator's focus comes after last month's cyberattack on the town of Peterborough that resulted in the theft of $2.3 million in taxpayer dollars, almost all of which was converted into cryptocurrency, which, according to the authors of the bill, rendered it nearly impossible to recover. Additionally, during the confirmation hearing for Treasury Secretary Janet Yellen, Senator Hassan pressed for the agency to take action against illegal uses of cryptocurrency.

Blockchain technology

Congresswoman Doris Matsui (D-CA), Co-Chair of the Congressional High Tech Caucus and Vice Chair of the House Energy and Commerce Communications and Technology Subcommittee, as well as Congressman Brett Guthrie (R-KY) and Senators Ed Markey (D-MA) and Todd Young (R-IN), reintroduced the Blockchain Promotion Act of 2021 (H.R. 3612). This legislation would establish a working group of stakeholders across the federal government and private industry to establish a common definition of blockchain. Specifically, the Blockchain Promotion Act would direct the Department of Commerce to establish a blockchain working group to recommend a consensus-based definition of the technology. The working group would also consider recommendations for the National Telecommunications and Information Administration (NTIA) and Federal Communications Commission (FCC) to undertake a study that would examine the potential impact of blockchain on spectrum policy and opportunities for the adoption of blockchain to promote efficiencies within the federal government.

The Blockchain Technology Coordination Act of 2021 was reintroduced as H.R. 3543 by Congressman Darren Soto (D-FL) to establish a Blockchain Center of Excellence within the U.S. Department of Commerce. The office would oversee all non-defence-related deployment and activities related to blockchain technology within the federal government.

The Blockchain Regulatory Certainty Act (H.R. 5045) would provide clarity for blockchain innovators and a safe harbour for licensing and registration for certain non-controlling blockchain developers and providers of blockchain services. Congressman Tom Emmer (MN-06) reintroduced the bipartisan Blockchain Regulatory Certainty Act with Rep. Darren Soto (D-FL), legislation designed to remedy concerning FATF proposed guidance that threatens to stifle blockchain innovation in the United States and send it overseas. In 2021, the FATF issued draft guidance to expand the definition of VASP to include any provider that may develop or operate a decentralised finance (DeFi) platform, even if they have no interaction with users. This action, if implemented in the United States, would require many innovators and developers in the blockchain space who never transmit money or custody consumer funds to navigate the overburdensome and stifling U.S. money transmission system as well.

Digitising the U.S. dollar: CBDC considerations for the U.S.

Reps French Hill (R-AR) and Jim Himes (D-CT) announced the introduction of the bipartisan H.R. 3506, the 21st Century Dollar Act. This legislation requires the Department of the Treasury, in coordination with the Federal Reserve, to implement a strategy for the dollar to ensure it be maintained as the primary global reserve currency. A reserve currency is held by central banks around the world in large quantities and is used to conduct international trade and financial transactions. This legislation outlines that the dollar calls for: (1) deep, open, and transparent financial markets; (2) continuous improvements to domestic and international payment methods that facilitate dollar transactions; (3) sound

macroeconomic governance and rules-based system of international trade; and (4) clear and realistic objectives in the deployment of financial restrictions arising from national security considerations. The legislation requires that the U.S. Treasury and the Federal Reserve create a policy that is reflective of these ideals and submit a report to Congress. The bill also requires reporting on any risks to the dollar posed by the internationalisation of the renminbi – China's official currency.

Congressman Hill also introduced the Central Bank Digital Currency Study Act of 2021 (H.R. 2211), which will direct the Board of Governors of the Federal Reserve System to conduct a study on CBDCs, and for other purposes. The bill outlines how a January 2021 survey by the Bank for International Settlements (BIS) found that 86 per cent of central banks, representing countries with close to 72 per cent of the world's population and 91 per cent of global economic output, are currently or will soon be engaged in work relating to CBDC, with almost three-quarters of such central banks having moved beyond the research of CBDC to experimentation, proof of concept, or testing activities. Also, since December 2016, the European Central Bank and the Bank of Japan have conducted a joint research project named "Project Stella", which aims to conduct experimental work and conceptual studies exploring the opportunities of digital ledger technologies and challenges for the future of financial market infrastructures, including CBDCs.

Additionally, since 2014, the People's Bank of China has conducted research and development activities for a CBDC, and in October 2020, launched a digital yuan pilot programme in Shenzhen. Back in the United States, as of August 2020, the Federal Reserve Bank of Boston announced a collaboration with the Digital Currency Initiative at MIT to perform technical research related to a CBDC. Also, in October 2020, the Financial Stability Board, in coordination with the BIS's Committee on Payments and Market Infrastructures, released a report to provide a roadmap for enhancing cross-border payments, including an exploration of new payment infrastructures presented by CBDCs. Finally, in January 2020, the BIS announced that the Bank of England, the Bank of Canada, the Bank of Japan, the European Central Bank, Sveriges Riksbank, the Swiss National Bank, and the BIS had formed a group to share information on the potential uses of CBDC in the central banks' jurisdictions, as well as information on potential economic, functional, and technical design choices. Additionally, according to data from the International Monetary Fund, as of the third quarter of 2019, the U.S. dollar share of global currency reserves totalled $6.75 trillion, or 61.78 per cent of all allocated reserves, and the standing of the U.S. dollar as the world's predominant reserve currency enables the United States to use economic sanctions as a foreign policy tool. Finally, according to a 2018 report by the Board of Governors of the Federal Reserve System, cash continues to be the most frequently used payment instrument, representing 30 per cent of all transactions and 55 per cent of transactions under $10, with 77 per cent of those transactions made in person.

As the Federal Reserve System is responsible for, among other things, conducting U.S. monetary policy, promoting the stability of the financial system, supervising financial institutions to ensure safety and soundness, ensuring the safety and efficiency of payment systems, and issuing and circulating Federal Reserve notes, the bill suggests a "Sense of Congress" that the Board of Governors should continue to conduct research on, design, and develop a CBDC that takes into account its impact on consumers, businesses, the U.S. financial system, and the U.S. economy, including the potential impact of a CBDC on monetary policy; and the United States should strive to maintain its leadership in financial technology and ensure that the U.S. dollar remains the predominant reserve currency in the world economy.

The bill calls for a study by the Office of the Comptroller of the Currency, the FDIC, the Department of the Treasury, the SEC, and the CFTC, to determine the impact of the introduction of a CBDC. Different concerns related to the impact include: (1) consumers and small businesses, including with respect to financial inclusion, accessibility, safety, privacy, convenience, speed, and price considerations; (2) the conduct of monetary policy and interaction with existing monetary policy tools, the effectiveness of U.S. economic sanctions programmes and the status of the U.S. dollar as a reserve currency, the U.S. financial system and banking sector, including liquidity, lending, and financial stability mechanisms, the U.S. payments and cross-border payments ecosystems, including the FedNow Service, and compliance with existing AML/BSA obligations, illicit financing, and related laws and regulations, and electronic recordkeeping requirements, data privacy and security issues related to CBDC, including transaction record anonymity and digital identity authentication; (3) the international technical infrastructure and implementation of such a system, including with respect to interoperability, cybersecurity, resilience, offline transaction capability, and programmability; (4) the likely participants in a CBDC system, their functions, and the benefits and risks of having third parties perform value-added functions, such as fraud insurance and blocking suspicious transactions; and (5) the operational functioning of a CBDC system, including (a) how transactions would be initiated, validated, and processed, (b) how users would interact with the system, and (c) the role of the private sector and public-private partnerships.

U.S. Senators Mark Warner (D-VA) and Bill Hagerty's (R-TN) Communist China's Digital Currency – National Security Risks Act has been included in the Intelligence Authorization Act for FY22 as marked up by the Senate Select Committee on Intelligence. The bill requires the Biden Administration to report on the potential short-, medium-, and long-term national security risks to the United States associated with Communist China's creation and use of an official digital currency. The bill requires reporting specifically on risks arising from the Chinese Communist Party's (CCP) potential surveillance of financial transactions, risks related to security and illicit finance, and risks related to economic coercion and social control by the CCP. The Intelligence Committee has included this requirement for a report in its Intelligence Authorization Act.

Since 2014, the CCP has been developing a digital version of its currency and may have the most advanced state-sponsored digital currency among major economies in the world. CCP officials are now ramping up for wider-spread deployment of its digital currency by the 2022 Winter Olympics. This will provide the CCP with additional information about financial transactions and economic activity, and could be used to evade U.S. sanctions. Now is the time for the U.S. intelligence community to act and inform us of their assessment of the different national security risks to the United States so that Congress may act appropriately and protect the U.S. dollar's position as the world's reserve currency – a key ingredient of the United States' global leadership. Senators Marsha Blackburn (R-TN), George Wicker (R-MI) and Cynthia Lummis (R-WY) also wrote a letter[26] to the United States Olympic & Paralympic Committee requesting that the teams boycott the use of the CCP digital currency while participating in the Olympic Games on Mainland China.

The Automatic BOOST to Communities Act of 2021 (H.R. 1030) is a bill that directs the Treasury Secretary to establish the Boost Communities Program to provide monthly payments to the United States' consumers during the COVID-19 pandemic to recover from the emergency. The bill is sponsored by Congresswoman Rashida Tlaib (D-MI), with co-sponsors including Congresswoman Pramila Jayapal (D-WA), Congressman Jesús García (D-IL), Congresswoman Eleanor Holmes Norton (D-DC), Congresswoman Alexandria

Ocasio-Cortez (D-NY), Congresswoman Ilhan Omar (D-MN), Congresswoman Ayanna Pressley (D-MA) and Congresswoman Cori Bush (D-MO).

The bill provides at the end a Sense of Congress that establishes FedAccounts and Treasury-administered eCash wallets, as well as describing a digital dollar account wallet provided by the Treasury and a digital dollar account available at the Federal Reserve. This type of "digital dollar" focuses less on the creation of a CBDC that would be an extension of the two-tier system that is currently in operation today, and focuses instead on more direct retail services offered by the Federal Reserve in tandem with the U.S. Treasury that would direct the supervision over the digital dollar account wallets.

Congressman Emmer just recently sent a letter[27] to Federal Reserve Chair Jay Powell that was signed by Congressman Darren Soto (D-FL), Congressman Ro Khanna (D-CA), Congressman Eric Swalwell (D-CA), Congressman Frank Lucas (R-OK) and Congressman Glenn "GT" Thompson (R-PA), which asks the Fed to respond on areas related to how it is looking to provide regulatory clarity for digital assets and what steps it is taking to provide guidance to banks that want to custody digital assets or offer cryptocurrency.

Finally, as previously mentioned, the letter challenges the notion that the Fed Chair stated to the Committee on July 14, 2021 that the strongest argument in favour of a U.S. CBDC is that it eliminates the need for cryptocurrencies and stablecoins. Specifically, the Fed Chair stated: "[Y]ou wouldn't need stablecoins, you wouldn't need cryptocurrencies if you had a digital U.S. currency – I think that's one of the stronger arguments in its favor."

However, on March 22, 2021, the Fed Chair said about Bitcoin: "It is essentially a substitute for gold rather than the dollar." The letter asks him to explain the contradiction in these statements given that a dollar CBDC would not be a substitute for a gold-like cryptocurrency. Additionally, since cryptocurrency networks do not merely facilitate value transfer, but also make possible myriad applications – from decentralised identity to decentralised file storage – the letter asked whether he believes a CBDC would make these applications, and the cryptocurrencies that power them, obsolete.

Conclusion

In conclusion, the 25 bills that have been introduced in the 117th Congress show a strong desire and interest by legislators to provide regulatory clarity to the blockchain and cryptocurrency industry, as well as how policymakers grapple with new policy challenges such as ransomware and sanctions issues. During the remainder of 2021 and 2022, there is strong potential that a great deal of the foundation will be laid that will help create much of the direction for how cryptocurrencies and blockchains are regulated, as well as what the future holds for CBDCs in the United States.

* * *

Endnotes

1. https://www.congress.gov/117/bills/hr3723/BILLS-117hr3723rfs.pdf.
2. https://www.congress.gov/117/bills/hr5082/BILLS-117hr5082ih.pdf.
3. https://www.congress.gov/117/bills/hr5083/BILLS-117hr5083ih.pdf.
4. https://www.congress.gov/117/bills/hr4741/BILLS-117hr4741ih.pdf.
5. https://www.congress.gov/117/bills/hr3638/BILLS-117hr3638ih.pdf.
6. https://www.congress.gov/117/bills/hr1602/BILLS-117hr1602rfs.pdf.

7. https://www.congress.gov/117/bills/hr808/BILLS-117hr808ih.pdf.
8. https://www.congress.gov/117/bills/hr296/BILLS-117hr296ih.pdf.
9. https://www.congress.gov/bill/117th-congress/house-bill/3684/text?q=%7B%22search%22%3A%5B%22infrastructure+investment+and+jobs+act%22%2C%22infrastructure%22%2C%22investment%22%2C%22and%22%2C%22jobs%22%2C%22act%22%5D%7D&r=1&s=3.
10. https://www.congress.gov/117/bills/hr154/BILLS-117hr154ih.pdf.
11. https://www.congress.gov/117/bills/hr3273/BILLS-117hr3273ih.pdf.
12. https://www.congress.gov/117/bills/s2666/BILLS-117s2666is.pdf.
13. https://www.congress.gov/117/bills/hr4451/BILLS-117hr4451ih.pdf.
14. https://www.congress.gov/117/bills/hr1628/BILLS-117hr1628ih.pdf.
15. https://www.hassan.senate.gov/imo/media/doc/sil21788.pdf.
16. https://www.congress.gov/117/bills/hr5101/BILLS-117hr5101ih.pdf.
17. https://www.congress.gov/117/bills/hr5100/BILLS-117hr5100ih.pdf.
18. https://www.congress.gov/117/bills/hr3639/BILLS-117hr3639ih.pdf.
19. https://www.congress.gov/117/bills/hr3612/BILLS-117hr3612ih.pdf.
20. https://www.congress.gov/117/bills/hr5045/BILLS-117hr5045ih.pdf.
21. https://www.congress.gov/117/bills/hr3543/BILLS-117hr3543ih.pdf.
22. https://www.congress.gov/117/bills/hr3506/BILLS-117hr3506ih.pdf.
23. https://www.congress.gov/117/bills/hr1030/BILLS-117hr1030ih.pdf.
24. https://www.congress.gov/117/bills/hr2211/BILLS-117hr2211ih.pdf.
25. https://www.congress.gov/117/bills/s2543/BILLS-117s2543is.pdf.
26. https://www.blackburn.senate.gov/services/files/95810475-939F-48C7-BDCE-5137DBBCECF2.
27. https://emmer.house.gov/_cache/files/f/4/f45a6df3-66b8-451a-b20f-accaec068e96/C1AD7E0FC99A66028BA6378A5A22133C.congressional-letter-to-powell.pdf.

Jason Brett
Tel: +1 703 215 5213 / Email: jason@valuetechnology.org

Jason Brett formerly served as a regulator at the FDIC during the last financial crisis. Additionally, he has extensive experience in developing and implementing successful governmental affairs programmes for various companies, including clients of Key Bridge Advisors. While serving as Policy Director for the blockchain technology company ConsenSys, he was responsible for their domestic and international policy during a key period of their growth. Jason has also worked as a consultant at Booz Allen Hamilton, and the Operations Director for the Chamber of Digital Commerce. He is the Founder and CEO of the Value Technology Foundation, a non-profit technology think tank. He is also a forbes.com contributor who writes on policy issues related to cryptocurrency and blockchain. Jason holds an M.B.A. from American University and a Bachelor's degree from Cornell University.

Whitney Kalmbach
Tel: +1 808 222 3084 / Email: whitney@valuetechnology.org

Whitney Kalmbach is a former US Naval Intelligence Officer with experience working in financial services, military contracting, business development, and consulting at JPMorgan Chase, Raytheon, and Deloitte. Her consulting work at Key Bridge Advisors has helped clients pursue business development opportunities and make key strategic decisions. She has also been instrumental in launching and growing the operations of the Value Technology Foundation, a non-profit think tank dedicated to blockchain for which she serves as CEO. Whitney holds an Executive M.B.A. from the Wharton School of the University of Pennsylvania, and a Bachelor's degree from Princeton University.

Value Technology Foundation

1300 I Street N.W., Suite 400E Washington, D.C., USA
Tel: +1 703 215 5213 / URL: www.valuetechnology.org

Six years of promoting innovation through education:

The blockchain industry, law enforcement and regulators work towards a common goal

Jason Weinstein & Alan Cohn
The Blockchain Alliance

Criminal use of technology

The crypto-asset industry has gone through substantial change since Bitcoin and other cryptocurrencies began experiencing wider use and adoption. However, questions concerning criminal use of cryptocurrencies and other types of crypto-assets persist, and indeed, seem to resurface with the introduction of each new advancement in technology. Fundamentally, crypto-assets have the potential to change the financial services industry in ways that provide greater functionality and access to a wider range of people than ever before. However, industry and government must continue to work together to curb criminal use of the technology.

Even though Bitcoin was introduced over 10 years ago, when many people think of "Bitcoin" or other cryptocurrencies, they often think of crime. From now-historical events such as the Mt. Gox hack and the Silk Road case to the use of cryptocurrencies in ransomware attacks, criminal use of cryptocurrency often prompts examination of the crypto-asset industry as a whole.

However, for the entrepreneurs, engineers, venture capitalists and bankers who are pouring their time, energy, and money into cryptocurrency- and crypto-asset-related businesses, the potential for the technology to bring about a revolution in financial innovation and inclusion, and to improve people's lives, is undeniable. And they know that contrary to popular belief, in the overwhelming number of cases, this technology is friendlier to law-enforcers than it is to law-breakers.

Blockchain technology uses cryptography to verify and confirm all transactions and then records those transactions on a searchable public ledger. It is often said that cryptocurrencies represent just the first "app" for blockchain technology. There are endless other possibilities for that technology – from securities and commodities trading, to decentralised financial applications, to supply chain management, to intellectual property rights and the use of non-fungible tokens ("NFTs"), to identity management and security, to real estate to government services, just to name a few – that could transform the way the world does business, much like the internet did over 20 years ago.

It is a fact of life in law enforcement that criminals are always among the first adopters of any novel technology that works. And law enforcement has a long history of adapting in order to pursue criminals who use "new school" technology to commit "old school" crimes. From beepers to email to online chat to Skype to social networking, law enforcement consistently has had to evolve as new technology designed for legitimate purposes is used to facilitate criminal activity. Cryptocurrencies and crypto-assets represent just the latest example.

While there is of course a vast amount of criminal activity taking place via the internet, none of us thinks of the internet as the "computer network of criminals". That is because the vast majority of commercial activity over the internet is legitimate, whereas illicit activity

facilitated by the web represents just a small portion of what happens on the internet every day. Similarly, cryptocurrencies should not be thought of as "currencies of criminals", because illicit transactions, while they exist, account for only a minute portion of the activity involving this new technology. Moreover, this technology has more potential to help fight crime than it does to facilitate it.

Proactive engagement by industry

Recognising a shared interest in helping combat criminal exploitation of this revolutionary technology, six years ago the blockchain and cryptocurrency industry proactively approached law enforcement and regulatory agencies and offered to help educate these agencies about how cryptocurrencies work, provide technical assistance and an understanding of industry best practices, and foster an open dialogue about issues of common concern. Under the leadership of the Chamber of Digital Commerce and Coin Center, the industry established the Blockchain Alliance, a non-profit organisation administered by Steptoe & Johnson LLP that serves as a forum for engagement between the blockchain industry and law enforcement and regulatory agencies. Since its founding in 2015, the Blockchain Alliance has grown to include approximately 120 blockchain and cryptocurrency companies and law enforcement and regulatory agencies in the U.S. and around the world, including Europol and Interpol and government authorities in Europe, Latin America, Africa, Asia, and Australia. In 2020, the Blockchain Alliance added programming specifically for compliance officials at the world's largest banks, helping to introduce, or reintroduce, those institutions to the blockchain and cryptocurrency industry and to the features and compliance solutions that exist to help conduct transactions utilising crypto-assets in a safe, efficient, and compliant manner.

Through the Blockchain Alliance, some of the brightest minds in the industry are working proactively with law enforcement and regulatory agencies to combat criminal activity involving this new technology, in an effort to promote public safety and a pro-innovation regulatory environment. The Blockchain Alliance convenes regular virtual meetings to discuss trends in the industry and tools for combatting criminal activity. The Alliance has conducted educational programmes for over 1,000 law enforcement officers and regulators from more than 35 countries. These educational programmes have covered a range of topics from tracing cryptocurrency transactions, to mixers and tumblers, to privacy coins, to utilising blockchain technology to prevent and combat child exploitation. Finally, the Alliance provides mechanisms for law enforcement and regulatory agencies to connect directly with industry on matters of common concern.

Tracing the flow of funds

One of the main misconceptions Blockchain Alliance members have worked to correct is that crypto-asset transactions are anonymous. The reality is that the technology has significant benefits for investigators seeking to "follow the (digital) money". Having a public, traceable, immutable, borderless ledger of every transaction ever conducted allows law enforcement to trace the flow of funds involving an investigative target anywhere in the world in a way that would not be possible with cash or many other types of financial instruments. And industry has developed software tools for connecting crypto-asset addresses to a particular user – similar to the challenge law enforcement has faced for years trying to identify anonymous hackers and other cybercriminals – and those tools are continually improving, as well as expanding for use with respect to other cryptocurrencies. Those same types of tools allow crypto-asset exchanges and others to better identify suspicious actors and transactions as part of their anti-money laundering ("AML")

compliance programmes. Under the circumstances, criminals should be running, not walking, away from using Bitcoin and other types of cryptocurrencies.

Growth of regulatory regimes

While it is often said that cryptocurrencies and blockchain technology are unregulated, nothing could be further from the truth. Numerous federal and state agencies in the U.S., as well as agencies in other countries, regulate applications for this technology in some fashion. But the disparate approaches taken by different countries, or even by different agencies within the U.S., have led to confusion on the part of blockchain companies about the jurisdictions and regulatory regimes to which their products and services may be subject.

Many jurisdictions, even within the U.S., regulate cryptocurrency activities like the exchange of cryptocurrency to fiat, or cryptocurrency to cryptocurrency, differently. Europe has now adopted regulation to include cryptocurrency companies, like exchanges, within the scope of the 6th Anti-Money Laundering Directive, and the European Council is conducting a first reading of the European Commission's proposed Regulation on Markets in Crypto-Assets ("MiCA") that will form part of its Digital Finance Strategy. Some exchanges offering services that do not clearly fit in the current regulatory regime have voluntarily developed robust procedures in order to verify their customers' identity and source of funds. These "on-ramps" and "off-ramps" to the cryptocurrency economy provide law enforcement, regulatory agencies, and traditional financial institutions with insights concerning the cryptocurrency economy as well as places to check and monitor transactions back and forth between cryptocurrencies and fiat currencies. Indeed, key trendlines indicate that while criminals continue to look for ways to evade AML measures, those measures are getting more stringent and more effective. For example, the blockchain forensics and cryptocurrency analytics provider CipherTrace, a Blockchain Alliance member, estimates that crypto-related crime has fallen from $4.5 billion in 2019 to $1.9 billion in 2020, a reduction of 57%.[1]

Moving forward through continued engagement between industry and government

Clear "rules of the road" are important – they help companies follow the law, they help regulators enforce it, and they help industry and government work together to protect public safety. But it is critical that these regulatory regimes be developed with input and insights from industry experts.

In order to ensure the growth of the industry while also protecting consumers and preventing money laundering, a pro-innovation approach to regulation is needed. Positive and proactive engagement by industry with law enforcement and regulators, through the Blockchain Alliance and otherwise, has been critical to the growth of this sector to date. Continued engagement of this type will be even more important going forward, as industry seeks to foster an approach to lawmaking and rulemaking that encourages, rather than stifles, innovation. Only then can the full potential of blockchain technology be realised.

* * *

Endnote

1. CipherTrace, February 2021 Cryptocurrency Crime and Anti-Money Laundering Report, https://ciphertrace.com/2020-year-end-cryptocurrency-crime-and-anti-money-laundering-report/.

Jason Weinstein, Director
Tel: +1 202 429 8061 / Email: jweinstein@steptoe.com

Jason Weinstein is Partner at Steptoe & Johnson LLP, co-chair of the firm's Blockchain and Cryptocurrency practice, and Director to the Blockchain Alliance. He has represented just about every type of participant in the blockchain ecosystem and is widely recognised as one of the leading defence attorneys in government enforcement matters relating to cryptocurrencies. Jason previously served as deputy assistant attorney general in the Department of Justice's Criminal Division, where he supervised the computer crime and organised crime sections, and oversaw numerous investigations involving the use of digital currencies. Jason serves on the advisory boards of Coin Center and the Chamber of Digital Commerce. He also serves as an advisor to Bitfury, the leading full-service blockchain technology company and one of the largest private infrastructure providers in the industry.

Alan Cohn, Counsel
Tel: +1 202 429 6283 / Email: acohn@steptoe.com

Alan Cohn is Partner at Steptoe & Johnson LLP, co-chair of the firm's Blockchain and Cryptocurrency practice, and Counsel to the Blockchain Alliance. Alan counsels companies on cybersecurity, blockchain and distributed ledger technology, and national security issues. Alan is ranked among the top U.S. lawyers in Blockchain and Cryptocurrencies by *Chambers USA* (2019–2021), where he is noted for his "tremendous depth of expertise in regulatory issues facing blockchain platforms and cryptocurrencies". He previously served in senior policy and management positions at the U.S. Department of Homeland Security for almost a decade, most recently as the Assistant Secretary for Strategy, Planning, Analysis & Risk and second-in-charge overall of the DHS Office of Policy. Alan also serves as an advisor to several technology companies.

The Blockchain Alliance

1330 Connecticut Avenue, NW, Washington, D.C. 20036, USA
URL: www.blockchainalliance.org

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

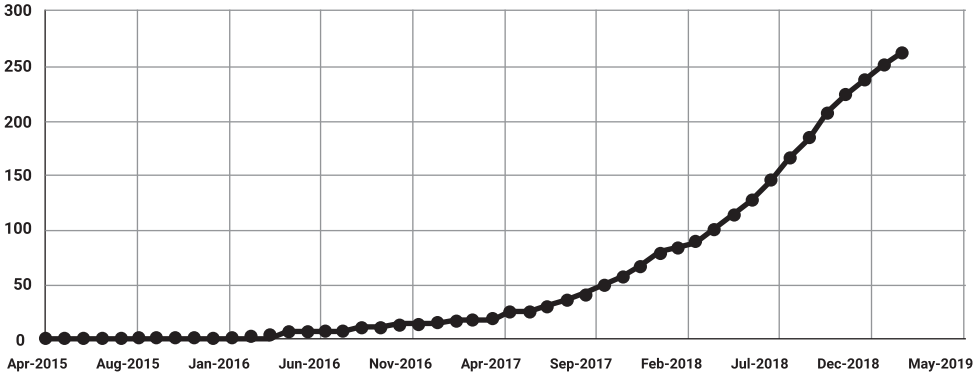
Since Satoshi Nakamoto published the Bitcoin whitepaper in 2008,[2,3] the number of worldwide blockchain patent applications has steadily risen:

Year	Patent Application Filings (Worldwide)
2016[4]	895
2017[5]	1,631
2018[6]	4,673
2019[7]	5,800
2020[8]	9,415

Notably, two Chinese entities (Ant Group and Ping An Group) filed the greatest number of blockchain patent applications in 2020, accounting for nearly 20% of all filed applications.[9] The top four entities that filed for a blockchain patent in 2020 were all based in China.[10]

The number of issued U.S. patents has likewise risen over time. In 2015, the United States issued only two patents relating to blockchain. In 2018, there were 170 such patents. In 2019, there were 659 such patents, growing to 1442 in 2020. The chart below depicts the rapid growth of U.S. blockchain patents:

Blockchain Patents Issued Over Time [Monthly Cumulative]



The largest holders of these U.S. blockchain patents as of Q3 of 2021 are shown below:[11]

Entity	Industry	No. of U.S. Blockchain Patents
Advanced New Technologies	Technology	453
IBM	Technology	341
Bank of America	Finance	89
Dell Technologies	Technology	57
Capital One	Finance	54
Accenture	Consulting	49

Entity	Industry	No. of U.S. Blockchain Patents
Mastercard	Finance	45
State Farm	Finance	36
American Automobile Assc.	Finance	33
Microsoft	Technology	33
Coinplug	Technology	31

Because blockchain technology assists in the efficient and secure transfer of digital assets, it is no surprise that the financial and technology industries currently dominate the blockchain patent space. Technology companies like IBM[12] and Dell[13] 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, and 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.

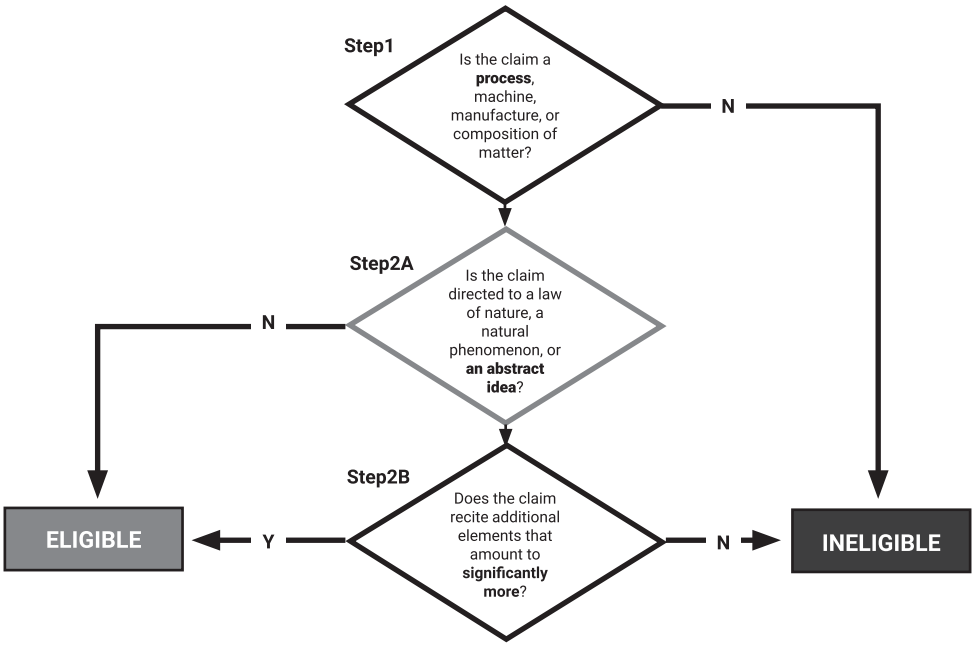
Accordingly, various companies and entities are devoting considerable time and resources to refining and revising the manner in which the traditional banking industry effectuates such monetary transactions. Entrepreneurial companies are inventing unique systems for effectuating asset transfers between 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.[14] 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.

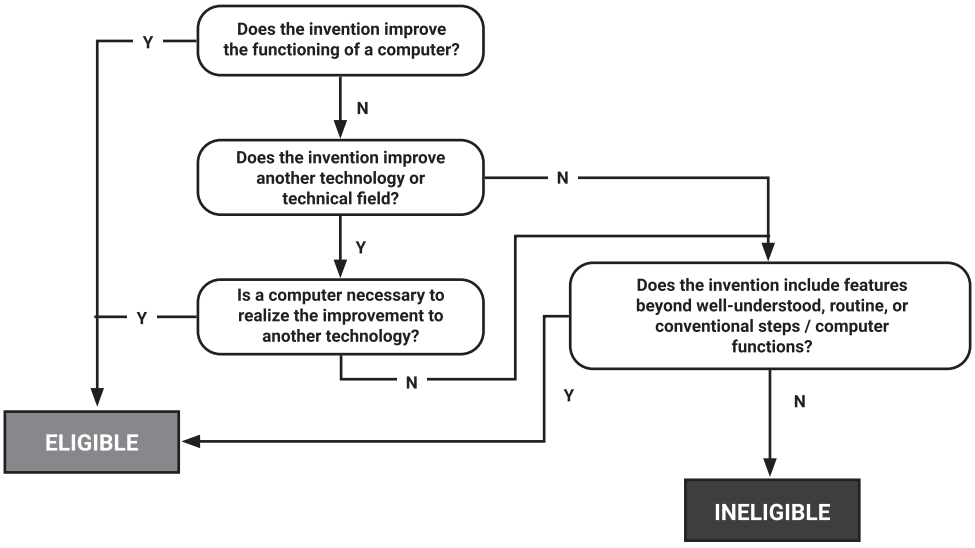
The following flowchart defines the manner in which the patentability of subject matter should be analyzed with respect to the *Alice* decision:



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.

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. However, the prudent company also would 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. Erich 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.[15] 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.[16] 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 "The impact of open-source software" section below, or by FRAND licensing obligations, as per our discussion in the "The role of industry standards" section below. 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.[17]

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**. While there are many blockchain patents and patent applications, they number in the hundreds, not the thousands. As such, if committed, our hypothetical company can review patent applications as they are published (18 months after filing) and when patents issue (on average three to four years after filing). 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,[18] public Ethereum,[19] and Hyperledger,[20] and portions of the software code bases for Enterprise Ethereum[21] and Corda,[22] 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.[23] 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,[24] 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"),[25] because this license (and variants) governs large portions of the Ethereum code base;[26] and the Apache 2.0 license ("Apache License"),[27] because this license governs open-source software provided via the Hyperledger, Corda, and Enterprise Ethereum platforms.[28] 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,[29] 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.[30] 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.[31] 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.[32] 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;[33] 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.[34] 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.[35]

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.[36] 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.[37] Industry players collaboratively develop these technical specifications in a Standards Setting Organization ("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.[38]
- 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;[39] and (2) Project 825 to develop a guide for interoperability of blockchains for energy transaction applications.[40]
- 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.[41]
- Hyperledger is a blockchain standard project and associated code base hosted by the Linux Foundation that focuses on finance, banking, the Internet of Things and manufacturing.[42]
- 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").[43]

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."[44] 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.[45] 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.[46]

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://blogs.thomsonreuters.com/answerson/in-rush-for-blockchain-patents-china-pulls-ahead.
5. https://blogs.thomsonreuters.com/answerson/in-rush-for-blockchain-patents-china-pulls-ahead.
6. https://www.lexology.com/library/detail.aspx?g=6aab712d-2ce9-401f-b37c-bffbe2aadf5f.
7. https://finance.yahoo.com/news/chinese-tech-giants-tencent-alibaba-154422979.html.
8. https://cointelegraph.com/news/chinese-holding-firm-ping-an-overtakes-tencent-in-blockchain-patents-race.
9. https://cointelegraph.com/news/chinese-holding-firm-ping-an-overtakes-tencent-in-blockchain-patents-race.
10. https://cointelegraph.com/news/chinese-holding-firm-ping-an-overtakes-tencent-in-blockchain-patents-race.
11. https://www.ipwatchdog.com/2020/12/04/the-blockchain-patent-landscape-shows-accelerating-growth; and https://harrityllp.com/titans-of-technology-blockchain-the-top-companies-in-blockchain-patents-2021/.
12. https://www.ibm.com/blockchain.
13. https://www.delltechnologies.com/en-us/perspectives/tags/blockchain.
14. *Alice Corp. v. CLS Bank Int'l*, 134 S. Ct. 2347 (2014).
15. 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/.
16. 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 . . .").
17. https://blog.coinbase.com/how-we-think-about-patents-at-coinbase-26d82b68e7db.
18. *See* http://www.Bitcoin.org.
19. L. Zeug, "Licensing" (September 4, 2016), located at https://github.com/ethereum/wiki/wiki/Licensing.
20. "About Hyperledger," located at https://www.hyperledger.org/about.
21. 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/.
22. "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/.
23. R. Brown, "Corda: Open Source Community Update" (May 13, 2018), located at https://medium.com/corda/corda-open-source-community-update-f332386b4038.
24. Bitcoin software, for example, is licensed under the permissive MIT License. *See* http://www.Bitcoin.org; https://opensource.org/licenses/MIT.
25. GPLv3 license, located at https://www.gnu.org/licenses/gpl-3.0.en.html.
26. 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.
27. Apache 2.0 license, located at https://www.apache.org/licenses/LICENSE-2.0.
28. 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/.

29. 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).
30. For convenience, the code the developer is required to open-source in this manner is referred to as "Derivative Code."
31. GPLv3, sec. 11 (Patents).
32. GPLv3, sec. 10 (Automatic Licensing of Downstream Recipients).
33. 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.
34. Apache 2.0, sec. 3 (Grant of Patent License).
35. 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/.
36. 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/.
37. 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.
38. https://www.iso.org/committee/6266604.html.
39. http://standards.ieee.org/develop/project/2418.html.

40. http://standards.ieee.org/develop/project/825.html.
41. https://bita.studio.
42. https://www.hyperledger.org.
43. 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.
44. 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).
45. Gruber, Harald, The Economics of Mobile Telecommunications (Cambridge University Press, 2005) at 35.
46. *Id*.

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

Ieuan Mahony is a partner in Holland & Knight's Boston office. He concentrates his practice in intellectual property (IP) licensing and development, data privacy and security, and information technology (IT). 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 Colandreo is a partner in Holland & Knight's Boston office. Mr Colandreo serves as the National Patent Practice Leader and is a member of the Intellectual Property Group. A registered patent attorney, Mr Colandreo focuses his practice on client management, general intellectual property prosecution, transactional work, litigation support, due diligence work, and utility and design patent opinion work. Prior to entering law school, Mr Colandreo worked as a systems/software engineer for Johnson Controls.

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

Jacob Schneider is an attorney in Holland & Knight's Boston office and is member of the firm's Intellectual Property Group. His practice focuses on patent, trademark, copyright and trade-secret litigation and licensing transactions. Mr Schneider has substantial knowledge in a wide variety of technologies and industries, including telecommunications, transportation, computer hardware/software, web/mobile applications, blockchain, voice-recognition, sporting equipment, gaming, toys and life sciences devices.

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 decade that has followed, Bitcoin and countless other open-source, decentralised protocols inspired by Bitcoin (for example, Ethereum and Litecoin) have come to represent a $2 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 Ravencoin, which are designed to facilitate various peer-to-peer activities, from decentralised software applications to "smart" contracts to digital collectibles, such as CryptoKitties. 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 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".

The regulatory treatment of cryptocurrencies and other digital assets

As discussed above, interests in investment funds themselves are securities; however, these funds may hold a variety of different assets in pursuing their respective strategies – from digital assets (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,[4] 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").[5] 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 asset's offering and sale, including the economic realities of the transaction.[6] 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.[7] 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 relief 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.[8] 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.[9]

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.[10] 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,[11] but does not include currencies or securities, which are classified as excluded commodities.[12] 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.[13] 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.[14] 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 advisor with the SEC unless such individual or entity qualifies for an exclusion from the definition or an exemption from the registration requirement.[15]

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[16] (the "custody rule") has detailed provisions applicable to any SEC-registered investment adviser deemed to have custody, as defined under the rule. Among other things, 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 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) excludes an entity from registration as an investment company 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 and launching 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").[17]

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.[18]

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.[19] 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; however, the SEC staff has acknowledged that such funds that are not exchange-traded may invest in certain types of Bitcoin futures contracts.[20] As the authors discuss in "*The Current State of U.S. Public Cryptocurrency Funds*", there have been a number of requests to list on national securities exchanges the shares of exchange-traded funds that invest directly in digital assets or in digital asset derivatives.[21] The SEC has repeatedly denied such requests, and in January 2018, the SEC's Division of Investment Management 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 legal 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) income from forks, airdrops or similar occurrences ("fork-type income") constitutes "unrelated business taxable income" (or "UBTI") for U.S. tax-exempt investors; (iii) fork-type income is subject to non-resident alien tax withholding;[29] and (iv) 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 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 U.S. Internal Revenue Code of 1986, as amended (the "Code"), provide that if interests in a partnership are traded on an established securities market or are readily tradable on a secondary market, 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 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, 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 (even where the activities of the fund do not constitute the conduct of a trade or business in the United States, such that a non-U.S. investor could conceivably invest directly in the fund), the use of an offshore

"blocker" corporation might be necessary to attract tax-exempt investors. In particular, uncertainty regarding whether fork-type income constitutes 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 calls into question whether such funds will be treated as PFICs.[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 Aug. 24, 2021) (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 Aug. 24, 2021).
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. SEC Release No. 81207, *Report of Investigation Pursuant to Section 21(a) of the Securities Exchange Act of 1934: The DAO* (Jul. 25, 2017).
5. *See*, *e.g.*, SEC Release No. 10445, *In the matter of Munchee, Inc.* (Dec. 11, 2017).
6. 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).
7. 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.
8. 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").
9. *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.
10. *See* 7 U.S.C. § 1a(9).
11. *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).
12. *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.

13. *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).
14. 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.'").
15. Investment advisers not registered with the SEC may be subject to registration with U.S. states.
16. 17 U.S.C. § 206(4)-2.
17. 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.
18. 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.
19. *See* 1940 Act § 3(c)(1)-(7).
20. *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". In addition, as this chapter was being finalised, SEC Chairman Gary Gensler indicated that the SEC might also be willing to approve an exchange-traded fund that invests in Bitcoin futures if it was structured as a registered investment company. *See* SEC Chairman Gary Gensler, Remarks Before the Aspen Security Form (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.").

21. Trevor Kiviat & Gregory Rowland, The Current State of U.S. Public Cryptocurrency Funds, *ICLG – Public Investment Funds* (2021 ed.), https://iclg.com/practice-areas/public-investment-funds-laws-and-regulations/1-the-current-state-of-u-s-public-cryptocurrency-funds (last visited Aug. 24, 2021).
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 Aug. 24, 2021).
24. *See* CFTC Rule 180.1.
25. 2014-1 C.B. 938.
26. Rev. Rul. 2019-24, 2019-44 I.R.B. 1044.
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 is U.S.- or foreign-source income, or whether it constitutes "fixed 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. 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 / Fax: +1 212 701 5800 / URL: www.davispolk.com

Not in Kansas anymore:
The current state of consumer token regulation in the United States

Yvette D. Valdez, Stephen P. Wink & Paul M. Dudek
Latham & Watkins LLP

Developing a framework for consumer tokens

The digital asset sector continues to evolve at a rapid pace. As SEC Commissioner Hester Peirce put it, the sector is "about as nimble as it gets."[1] In 2021, we have witnessed the explosion of decentralized finance, yield farming, and governance tokens. Non-custodial decentralized exchanges continue to experience substantial growth, with total exchange volume peaking at over $150 billion in Q2 2021. Non-fungible tokens (NFTs) went from crypto curiosity in 2020 to mainstream in 2021, with sales for individual NFTs and lines of collectibles smashing records each consecutive month. Besides their popularity as collectibles, NFTs have also taken hold in the blockchain-based gaming, metaverse and virtual worlds, and as collateral for borrowing and backing stablecoins

As the US Securities and Exchange Commission (the SEC) continues to pursue enforcement actions with respect to token offerings (while scrupulously avoiding giving regulatory guidance), the question on the minds of many entrepreneurs and their counsel is what the parameters are for the issuance and sale in the United States of "consumer" or "utility" tokens – those designed for use by consumers on a distributed platform and not intended to constitute securities.[2] While there appears to be a viable regulatory path to the issuance of consumer tokens that would not necessarily be viewed as "securities" subject to SEC oversight, the framework continues to suffer from a lack of definite regulatory parameters and bright line definitions. In this chapter, we discuss the legal issues surrounding such issuances under the US federal commodities and securities laws.

This chapter serves as an update to the previous edition and reflects our most current and up-to-date thinking and analysis regarding the development of consumer token sales.

Existing frameworks

The securities law framework

The SEC's approach to whether a digital asset sold in a token sale would be a security derives from its application of the test set forth in *SEC v. W.J. Howey Co.* (the *Howey* Test).[3] The *Howey* Test determines whether an asset constitutes an "investment contract," one of the enumerated types of instruments defined in the securities laws.[4] The test states that an investment contract involves (i) an investment of money, (ii) in a common enterprise, (iii) in which the investor is led to expect profits, (iv) derived from the entrepreneurial or managerial efforts of one or more third parties.[5] If the test is satisfied, it is immaterial whether the enterprise is speculative or non-speculative, or whether there is a sale of property with or without intrinsic value.[6] In short, the heart of the analysis is to focus on the economic reality of the arrangement in question.

In July 2017, the SEC applied the *Howey* Test to digital assets for the first time, and arrived at the conclusion that the sale of Decentralized Autonomous Organization (DAO) tokens, a digital asset, was an unregistered securities offering undertaken without a valid exemption from Section 5 of the Securities Act of 1933 (the Securities Act). The SEC made clear that to the extent instruments have the indicia of investment contracts, they should be offered and sold in compliance with the securities laws.

In its first enforcement action relating to the sale of digital assets, on December 11, 2017, the SEC issued an order instituting cease-and-desist proceedings to halt Munchee Inc.'s sale of tokens (the *Munchee* Order), having concluded that the sale was an unregistered securities offering. A key lesson of the *Munchee* Order was that despite the utility design features of the MUN Tokens, the manner in which the digital assets were offered to prospective investors, and the presence of investment intent on the part of participating investors, constituted material factors for the SEC in determining that the offering was a securities offering subject to the US federal securities laws.[7]

Following the *Munchee* Order, in a June 2018 speech, William Hinman, Director of the SEC's Division of Corporation Finance at the time, emphasized that digital assets need not always be securities. Rather, in addition to the underlying rights associated with such assets, he reiterated that the manner of sale and the reasonable expectations of the purchasers help determine whether a particular digital asset is a security. This is underscored by Director Hinman's reference to *Gary Plastic Packaging v. Merrill Lynch, Pierce, Fenner & Smith Inc.*,[8] in which the Court found that an offering of a certificate of deposit, which in and of itself is not a security, was subject to US federal securities laws because marketing efforts relating to the certificates centered on the establishment of a secondary market and the opportunity for purchasers to profit from the enterprise. In the case of nascent token platforms and networks, digital tokens sold in an offering by promoters to "develop the enterprise" will most often constitute securities because the value of the token will primarily derive from the entrepreneurial efforts of the enterprise's promoters. Nevertheless, Director Hinman noted that transactions involving digital assets on a sufficiently decentralized network do not otherwise have the indicia of securities transactions and do not give rise to the public policy concern of informational asymmetries between an investor and issuer, and thus may not trigger the application of US federal securities laws. Director Hinman reiterated these ideas in a May 2019 speech, stating that a potential pathway exists for a token that was once a security to transmute into a non-security.

In April 2019, the SEC staff issued a "Framework for 'Investment Contract' Analysis of Digital Assets" (the Framework) to assist market participants to assess whether a digital asset constitutes an investment contract.[9] In addition, the SEC staff also released two no-action letters relating to token offerings in 2019. The first (the Turnkey Letter) was in response to a proposed token offering by TurnKey Jet, Inc. (Turnkey Jet), an air carrier and air taxi service, and the second (the PoQ Letter) was in response to Pocketful of Quarters, Inc.'s (PoQ) proposed token offering.[10] Together, the Turnkey Letter, PoQ Letter and Framework emphasize that the analysis of whether a utility token constitutes an investment contract typically hinges on the third and fourth prongs of the *Howey* Test; in particular, whether the investors have an expectation of profits that will be derived from the managerial efforts of others. The Framework now serves as the principal source of guidance for analyzing whether a digital asset falls within the definition of a security.

To evaluate "reliance on the efforts of others," the Framework introduces the concept of an Active Participant (AP), defined as "a promoter, sponsor, or other third party . . . [that]

provides essential managerial efforts that affect the success of the enterprise, and investors reasonably expect to derive profit from those efforts." Determining the existence of an AP necessarily requires an analysis of each party's role in developing, maintaining or governing the network. The presence of an AP means it is more likely that profits are being derived from the efforts of others.

To analyze "reasonable expectation of profit," the Framework bases its evaluation on whether an asset conveys the "right to share in [an] enterprise's income." This factor should be unsurprising to issuers, as it derives from the reasoning in the *DAO Report*, which pointed to the dividend-like feature of DAO tokens in classifying them as securities. Continuing in the vein of the SEC's prior pronouncements, the guidance also looks to how the digital asset is marketed, whether "the digital asset is offered broadly" (*e.g.*, via secondary markets) "to potential purchasers as compared to being targeted to expected users of the goods or services or those who have a need for the functionality of the network," and whether "[t]he AP continues to expend funds from proceeds or operations to enhance the functionality or value of the network or digital asset." Such factors appear to focus on the more speculative aspects of issuances, such as where the use and value of the digital asset is connected to an undeveloped network, the success of which may likely be tied to the capital raised through the issuance itself. In addition, the Framework looks to whether the AP will receive or retain any of the digital assets, and the nature of purchasers' expectations with respect to the role of the AP and the ongoing viability of the digital asset itself.

In June 2019, the SEC sued Kik Interactive Inc. (Kik) for allegedly conducting an illegal $100 million securities offering of Kik's digital token, Kin.[11] In its complaint, the SEC alleged that Kik marketed Kin to investors as an investment opportunity, offered and sold Kin before it had any utility, retained a proportion of the tokens for Kik and promised investors that Kin would be listed on secondary markets. For the SEC, such features meant the Kin offering was a securities transaction and should have complied with registration requirements as prescribed by the securities laws.[12] In a press release,[13] Kik responded to the SEC's suit, citing similar arguments as those raised in its Wells submission[14] in December 2018. Specifically, Kik argued that the SEC's complaint is based on "flawed legal theory" and expands the *Howey* Test beyond its prescribed limits. In support of this position, Kik claimed that "the complaint assumes, incorrectly, that any discussion of a potential increase in value of an asset is the same as offering or promising profits solely from the efforts of another; that having aligned incentives is the same as creating a 'common enterprise'; and that any contributions by a seller or promoter are necessarily the ['essential'] managerial or entrepreneurial efforts required to create an investment contract."[15] Of course, in addition to proving instructive, the resolution of this case and these issues could provide useful judicial precedent.

In June 2020, a year after commencing the Kik lawsuit, the SEC announced a settlement with Telegram Group Inc. (Telegram) over charges that Telegram had violated securities laws when it offered and sold its unregistered "Grams" token in exchange for $1.7 billion from 175 initial purchasers.[16] The Telegram fact pattern is strikingly similar to Kik's, in that both are operators of messenger applications that sought to introduce a token into their messenger service by selling pre-functional tokens to initial purchasers and using the funds to develop their respective networks.[17] Prior to the settlement, the Court in the Southern District of New York had sided with the SEC in March 2020 and granted an injunction prohibiting Telegram from delivering Grams to the initial purchasers. The Court held that Telegram's scheme constituted an investment contract, requiring either registration or an applicable exemption

in order to comply with securities laws. As part of the settlement with the SEC, Telegram returned $1.2 billion to the initial purchasers and paid an $18.5 million penalty.

Some commentators had hoped Telegram's case would provide further clarity on the path tokens should take to not constitute securities. Unfortunately, those hopes were not met, but the Court provided a brief hint of what might be, noting:

> "Cryptocurrencies (sometimes called tokens or digital assets) are a lawful means of storing or transferring value and may fluctuate in value as any commodity would. In the abstract, an investment of money in a cryptocurrency utilized by members of a decentralized community connected via blockchain technology, which itself is administered by this community of users rather than by a common enterprise, is not likely to be deemed a security under the familiar test laid out in [*Howey*]. The SEC, for example, does not contend that Bitcoins transferred on the Bitcoin blockchain are securities."[18]

Token safe harbor proposal

In a February 2020 speech, Commissioner Peirce proposed a token safe harbor, which would provide network developers with a three-year grace period to achieve sufficient decentralization for their network following the issuance of unregistered tokens.[19] On April 13, 2021, she reissued[20] the proposal as Token Safe Harbor Proposal 2.0 (Proposal 2.0), in light of feedback received since the original release from the crypto community, securities lawyers, and members of the public.

The original Safe Harbor Proposal, as well as Proposal 2.0, provide a time-limited exemption for token-based projects that seek to raise capital to develop decentralized networks. Proposal 2.0 would also allow fledgling networks to operate unburdened by the onerous registration provisions of the US federal securities laws until they reached network maturity (defined as either decentralization or token functionality). Provided that certain standards and disclosure requirements are met, a three-year grace period would be granted to allow token developers to pursue "sufficient" decentralization of their network from the time of the first token sale. As a result, purchasers of the token would no longer reasonably expect that the value of their tokens was being driven by a person or group via managerial or entrepreneurial efforts.

Although the Proposals were floated by a single SEC Commissioner, they are nevertheless a positive development for such a discussion to be taking place, and would provide token holders with greater protection and transparency if adopted. Unfortunately, however, there has been little enthusiasm from Commissioner Peirce's fellow Commissioners and other regulators for establishing a safe harbor such as Proposal 2.0.

A note on custody (SEC)

For centralized exchanges and broker-dealers acting as custodians of digital asset securities, the SEC staff issued a joint statement[21] with the Financial Industry Regulatory Authority on July 8, 2019, highlighting the importance of compliance with Rule 15c3-3 under the Securities Exchange Act of 1934 (the Customer Protection Rule). The Joint Statement emphasized how digital asset securities, as opposed to traditional securities, are particularly susceptible to being lost due to cyberfraud, cybertheft, loss of a private key, or a faulty blockchain transaction.

In addition, the SEC issued a related statement[22] on December 23, 2020 ("Custody of Digital Asset Securities by Special Purpose Broker-Dealers") clarifying its position on how broker-

dealers can establish possession or control of digital assets in compliance with the Customer Protection Rule to mitigate the risk of the loss or theft. Digital asset securities, according to the Custody Statement, do not provide customers the protections offered by traditional securities infrastructure. The SEC stated that the traditional infrastructure "contains checks and controls that can be used to verify proprietary and customer holdings of traditional securities by broker-dealers, as well as processes designed to ensure that both parties to a transfer of traditional securities agree to the terms of the transfer." The Custody Statement lays out the minimum measures that broker-dealers must take to comply with the Customer Protection Rule when acting as custodians of digital asset securities. The guiding principle behind the measures is to mitigate the risk of the loss or theft of digital asset securities and the impact such an event would have on broker-dealers, their customers and counterparties, and other market participants.

The commodities law framework

The US Commodity Futures Trading Commission (the CFTC) regulates futures, options on futures, and swaps (*i.e.*, derivatives) on commodities (including crypto-assets) (collectively, Commodity Interests). While the CFTC does not have general regulatory jurisdiction and oversight with respect to spot crypto-asset markets, the CFTC does retain general enforcement authority to police against manipulation and fraud in the spot commodities markets (including spot crypto-asset markets).[23] In 2014, then-CFTC Chairman Timothy Massad observed that what the CFTC has referred to as virtual currencies are "commodities" subject to provisions of the Commodity Exchange Act, as amended (the CEA).[24] Since 2015, the CFTC has been active in bringing enforcement actions when virtual currency enterprises run afoul of regulatory requirements[25] and in the enforcement against fraud and manipulation in the virtual currency "spot" markets.[26]

In addition to transactions in Commodity Interests, the CFTC also regulates commodity transactions with retail customers that are entered into or offered on a leveraged, margined or financed basis as if they were futures contracts (the Retail Leveraged Rules). However, if a transaction results in "actual delivery" of the relevant commodity within 28 days, such leveraged transaction will not be subject to regulation as a futures contract. Crypto-asset markets have exhibited increasing use of leverage and margin for the trading of crypto-assets, and the application of the Retail Leveraged Rules to transactions in crypto-assets has been an area of CFTC regulatory and enforcement emphasis. The CFTC has finalized interpretive guidance (the Guidance) on what constitutes "actual delivery" in the context of crypto-assets that serve as a medium of exchange (*i.e.*, virtual currency),[27] providing two primary factors for what would constitute "actual delivery" for purposes of the Retail Leveraged Rules: first, the purchaser must have possession and control over the virtual currency; and second, the purchaser must be able to use the virtual currency in commerce.

A note on custody (CFTC)

On October 21, 2020, the CFTC's Division of Swap Dealer and Intermediary Oversight issued CFTC Staff Letter No. 20-34,[28] clarifying its views on the acceptance, holding, and reporting of virtual currency (*e.g.*, Bitcoin or Ether) in segregated accounts by futures commission merchants (FCMs) and the development of appropriate risk management programs in relation thereto. Specifically, the Advisory related to virtual currencies deposited by customers with FCMs in connection with physically delivered futures contracts or swaps. Due to the "custodian risk" associated with holding virtual currency as segregated funds, the Advisory lays out specific guidance for FCMs on virtual asset acceptance and custody, and their responsibility to implement appropriate policies, procedures, and oversight programs.

Pre-functional consumer token sales[29]

It is generally understood that sales of tokens to fund an AP's development of a token-based network are highly likely to constitute investment contracts, regardless of the form of instrument evidencing the sale. That is, the efforts of the AP remain central to the value of the instrument being sold, thus satisfying the *Howey* Test as an investment contract. As a result, in an effort to separate the pre-functional sale and the underlying consumer token, financing instruments – most prominently, the Simple Agreement for Future Tokens (the SAFT)[30] and other similar token presale instruments – were designed. The SAFT is a presale instrument in which the sale of the SAFT is explicitly a securities transaction that is usually sold in compliance with an exemption from registration (*i.e.*, Regulation D) that promises the later delivery of the underlying token upon launch of the network. While such instruments attempted to solve the securities law issues with presales by delaying delivery of the token until after the network is functional, they raised other significant concerns.[31]

Securities law issues

While the token presale instruments may postpone delivery until after the utility token is functional, they fail to address the status of the underlying tokens and the impact of the presale offering on the marketing of the underlying tokens. That is, by structuring the token presale as an investment opportunity, these instruments arguably imply that the underlying token is being purchased for investment rather than consumptive purposes. As a general matter, such instruments are generally sold under an exemption from registration to accredited investors who may have to represent that they are purchasing for investment purposes.[32]

SAFTs raise another related concern. As settlement of these instruments generally contemplates delivery of the token at network launch,[33] the delivery of tokens to SAFT holders generally occurred at the same time as broader distribution to the community via airdrop or similar method. This potentially also implicates the tokens being distributed to the community as securities because under the logic of *Gary Plastic* and the *Munchee* Order, the settlement of these instruments is not directed solely to consumers and thus could make the delivery of all tokens a securities transaction, not a consumer token launch.[34]

Recent examples of the unintended consequences of using token presale instruments can be seen in the SEC's actions against Kik and Telegram.[35] Kik and Telegram each offered and sold pre-functional tokens to accredited investors in private placements pursuant to Regulation D via token presale agreements. Despite this, the SEC's view was that the private nature of the sales of tokens under the token presale instruments was vitiated because these sales were part of schemes that involved token sales to the public and thus constituted a single plan of financing that did not qualify for the private placement exemption from registration under US securities laws. In its Kik complaint, the SEC noted that "Kik sold the Kin as part of a single plan of financing, for the same general purpose, at about the same time, without creating different classes of Kin[.]"[36] Similarly, in halting the delivery of Telegram tokens to the initial purchasers, the Court found that "the delivery of Grams to the Initial Purchasers, who would resell them into the public market, represents a near certain risk of future harm, namely the completion of a public distribution of a security without a registration statement."[37]

Commodities law issues

Beyond the securities law concerns, the SAFT, and other similar token presale instruments, also raise commodities law concerns. Because cryptocurrencies are commodities,[38] a

presale of consumer tokens through an instrument that provides the right to receive tokens in the future, or confers the right to exchange or convert such instrument into tokens that are not securities, may be a forward contract for the sale of a commodity or a commodity option, and subject to regulation by the CFTC as a swap, if an exemption is not available.

(a) Commodity forward contracts

Forward sales of commodities fall within the CEA's broad definition of "swap," which encompasses numerous types of derivatives, and are subject to regulation by the CFTC absent an applicable exclusion.[39] Notably, the sale of a non-financial commodity for deferred shipment or delivery is excluded from the swap definition, so long as it is intended to be physically delivered,[40] but provided such forward contract also qualifies as a commercial merchandising transaction (the Non-Financial Forward Contract Exclusion).[41] If such instruments are purchased by investors or speculators, they will not satisfy the requirement of the Non-Financial Forward Contract Exclusion because the purchasers are not "commercial market participants."[42] The CFTC has expressly stated that hedge funds, acting in their capacity as investors, are not commercial market participants.[43] As such, token presale instruments are effectively a prepaid forward contract of a commodity whereby parties have agreed a price or percentage discount on the token to be delivered at a later date. As discussed above, the many token presale agreements are (and continue to be) largely marketed to investors and not commercial market participants;[44] such investors would not be eligible for the Non-Financial Forward Contract Exclusion.

(b) Commodity options

More recent versions of token presale instruments have also included convertible features, which provide investors or the issuer, as applicable, a call or put right to deliver tokens upon the consummation of a token sale at an agreed price or discount. Such an instrument may constitute a commodity option and would be subject to CFTC regulation as a swap,[45] unless an exemption applies. Trade options are generally exempt from regulation by the CFTC, other than certain large trader reporting requirements and the CFTC's general anti-fraud and anti-manipulation enforcement authority (the Trade Option Exemption).[46] In order to qualify as a trade option and benefit from the Trade Option Exemption,[47] the commodity option in question must be: (i) intended to be physically settled if exercised; (ii) entered into with an offeror who is either an eligible contract participant (ECP)[48] or a producer, processor or commercial user of, or merchant handling, the commodity (or products or by-products thereof) that is the subject of the option, and such offeror is offering to enter into such option solely for the purposes related to its business as such; and (iii) entered into with an offeree who is either a producer, processor or commercial user of, or merchant handling, the commodity (or products or by-products thereof) that is the subject of the option, and such offeree is entering into such option solely for the purposes related to its business as such.

Unfortunately (as stated above in connection with the Non-Financial Forward Contract Exclusion), many of the token presale instruments are not offered to commercial market participants who would satisfy the "offeree" prong, even if the issuer of the instrument could satisfy the "offeror" prong. Additionally, even if such instruments are offered to "consumers," they would not necessarily satisfy the "offeree" prong of the Trade Option Exemption, unless such consumer could establish a nexus to a business activity. Accordingly, token presale investors are unlikely to qualify for the Trade Option Exemption.

(c) *Hybrid Instrument Exemption*

Furthermore, since token presale instruments may constitute or contain a commodity forward contract or commodity option and may not otherwise qualify for the Trade Option Exemption or the Non-Financial Forward Contract Exclusion, we also consider whether such instruments would meet the Hybrid Instrument Exemption (defined below) and, as a result, be exempt from commodities law regulation. Under CFTC Rule 34.2(a), a "hybrid instrument" is defined to include an equity or debt security with "one or more commodity-dependent components that have payment features similar to commodity futures or commodity options contracts or combinations thereof."[49] Under Section 2(f) of the CEA, a hybrid instrument that is "predominantly a security" is exempt from the provisions of the CEA if, among other things, the instrument is not marketed as a contract of sale of a commodity for future delivery (or option on such a contract) subject to the CEA (the Marketing Condition) (such exemption being the Hybrid Instrument Exemption).[50]

While token presale instruments may, in theory, be capable of qualifying for the Hybrid Instrument Exemption, because they are often primarily marketed to investors who themselves are solely or in large part motivated to purchase such instruments in order to receive the underlying commodity (*i.e.*, the token), such instruments will often fail to satisfy the requirements of the Marketing Condition of the Hybrid Instrument Exemption.[51]

(d) *Retail leveraged transactions*

Further still, under certain structures, network participants who are also functionally retail investors may wish to receive a token. Network participants may receive such tokens through the financing of a third party or the network platform itself. The recently issued Guidance with respect to Retail Leveraged Rules has clarified uncertainty over what delivery actually means in this context and stresses meaningful possession and control and the ability to use such token in commerce. In certain instances, neither utility nor control is practicable within a 28-day timeline. As a result, such token presale structures may be regulated as futures contracts.

(e) *Consequences of CFTC regulation*

Because such presale instruments may have an embedded swap, which does not qualify for an exemption from regulation by the CFTC (as discussed above), such presale instrument would be subject to the full swaps regulatory framework applicable to such instruments, or in the case of Retail Leveraged Rules, subject to regulation as a futures contract. In particular, in order to trade over-the-counter, swaps must be entered into between ECPs.[52] While some investors may qualify as ECPs, token issuers typically are early-stage companies that may not have at least $10 million gross assets, and as a result, would not satisfy the ECP test. A swap entered into by parties who are not ECPs would be in violation of the CEA and CFTC regulation. As a result, the contract could be rescinded and both parties could face penalties and sanctions for such actions.

Potential solutions available through traditional financing instruments

Traditional early-stage financing structures, such as preferred stock and convertible promissory notes,[53] are "tried and true" structures that generally exhibit the necessary flexibility to address the needs of early-stage companies/token issuers and token platforms. We believe these structures can be augmented to address investor demand for exposure to consumer tokens, while enabling the parties to comply with applicable securities and commodities laws. This can be achieved by providing investors with various combinations of token-related purchase, economic and voting rights.

First, the conversion and exchange rights featured in currently popular token presale instruments could be replaced with appropriately limited token sale participation and economic rights that reduce the regulatory risks associated with consumer token sales discussed above. For instance, the purchase right would not represent a conversion or exchange of the security, but would include these rights in addition to the rights granted to the holder of the securities. The exercise of such token sale participation rights could be limited to sales or distributions of the consumer tokens that would not be deemed to be securities transactions, such as when the network had achieved sufficient decentralization (although the challenges in defining an objective standard for this trigger may reduce the practicality of this option). The participation rights could also be limited to purchases for actual use, or limit the consumer tokens reserved for distribution or sale to investors, and require that any distributions or sales thereof occur in a manner that supports the broader consumer token-based network.

Instead of the inclusion of pre-negotiated token prices in such instruments, which – from a commodities law point of view – may increase the risk of being considered a commodity option because such pre-agreed price could be seen as a strike price, the participation rights could be coupled with "most-favored nation" (MFN) pricing provisions, guaranteeing certain investors the best token sale and distribution terms offered by the issuer to any other third party. These rights could also be supplemented with token economic rights that could be triggered *in lieu* of participation in the consumer token sale. For example, preferred stock could be issued with various rights tied to consumer token sales, such as pre-negotiated dividend or redemption rights, or a convertible promissory note under which the issuer pays a multiple of the note's aggregate principal amount or the note converts into preferred stock with dividend or redemption rights. Such token economic rights would have the goal of providing the investor with a similar economic outcome of participating in the consumer token sale. As a result, the careful balancing of such token sale participation and economic rights could provide issuers the flexibility to allow for the participation of investors eager to receive token economics while protecting the development of the underlying network and consumer tokens from the application of the securities laws.

Second, because consumer tokens and the corresponding network protocol often represent a significant portion of the value proposition associated with investing in such platforms, investors can reasonably expect to receive voting rights with respect to the creation and distribution of tokens by the issuer, including the right to approve the initiation of any offerings or distributions.[54] Eventually, as the pathway for consumer token sales becomes clearer, voting rights grants may be more narrowly tailored to only apply when such a sale does not meet certain specifications. In addition, investors may seek additional protections to prevent potential uses of the issuer's token-based network that circumvent their consumer token-related economic and participation rights.

Finally, these preferred stock and convertible promissory note structures may also be preferred from a commodities law perspective for several reasons. First, conferring future participation rights on an investor to participate in a token sale, or conferring economic rights to an investor in respect of future distributions, is not clearly a swap under the CEA and subject to CFTC regulation. Currently, no regulatory certainty exists as to the treatment of preferred stock and convertible promissory note structures with token participation rights, and it is unclear whether such participation rights would constitute swaps (or not) subject to CFTC jurisdiction. There is no strike price or final price differential that creates market risk that the CFTC would necessarily be incentivized to regulate in the commodity options market. Such token participation rights seek to reduce economic risk and loss attributable

to other token presale agreements. They afford the investor an MFN pricing provision to purchase the token at spot price, which is likely to reduce an investor's risk of loss. Accordingly, for the reasons set forth above, we believe such structures reduce regulatory risk of CFTC intervention, which is inherent in predecessor token presale instruments.

Furthermore, if a swap were deemed to exist, in such structures where the conditions of the Hybrid Instrument Exemption other than the Marketing Condition are satisfied, one could argue that – despite the associated consumer token rights – such instruments are "predominantly securities" and unlikely to run afoul of the Marketing Condition, because the commodity forward or option would be a small portion of the value of the instrument. Accordingly, it would be much harder to argue that such instrument was marketed as a swap or purchased by investors solely for the purpose of receiving the value provided by the swap component. That is, because the predominant value of the instrument is a traditional security providing specific rights with respect to the issuer – such as traditional preferred stock rights (*e.g.*, liquidation preference, dividends, anti-dilution protection) or traditional promissory note rights (*e.g.*, returns of principal, potential conversion into equity) – such consumer token presales could arguably fall outside some (if not all) of the CFTC regulatory regime by qualifying for the Hybrid Instrument Exemption or being excluded entirely from the swap definition.[55]

Of course, while each instrument would need to be analyzed on its own merits, we believe these alternate structures have great promise for addressing commodities law issues. At a minimum, they significantly mitigate the regulatory risks of the SAFT and other similar presale token structures; and at best may offer a clear path to avoid characterization as a swap subject to CFTC jurisdiction.

Importantly, even if these preferred stock and promissory note structures are not completely exempt from regulation as a swap, certain token projects and network participants may qualify for the Trade Option Exemption, giving further relief from CFTC regulatory requirements.

These structures are also preferred from a securities law perspective for many similar reasons – because the investor is receiving a more traditional security, the various rights they are purchasing are far less ambiguous, and appropriate disclosures regarding the material aspects of the investment are more easily crafted.

Please note that in collaboration with ConsenSys, we have offered up a convertible note tool that we believe addresses the concerns raised in this chapter.[56]

Enabling true consumer token sales

Once a platform and token protocol have been developed, the question remains whether a viable consumer token sale may be accomplished. The Framework identifies a number of factors centering around two main inquiries to help distinguish when digital assets transactions may be characterized as securities transactions.[57] First, the Framework emphasizes the necessity of the AP for the continued success of the enterprise. Second, the Framework emphasizes the expectations held by network participants with regard to the AP and the token. Critical in this inquiry is the nature of the marketing of the consumer token and its platform, and the nature of the purchasers.

We believe we can draw two concrete takeaways from the Framework and relevant legal decisions that bear upon this analysis. First, tokens offered in a manner intended to appeal to an investor's investment intent are more likely to trigger the application of the securities laws. Second, when the token-based network has developed to an extent that the

value of the tokens can no longer be perceived to be dependent upon the entrepreneurial or managerial efforts of such network's APs, token trading on that network may not be considered securities transactions. To date, Bitcoin and Ether are the only tokens that the SEC has explicitly confirmed meet this level of sufficient decentralization.

Features of established non-security virtual currencies

Two of the most widely held and well-known digital assets – Bitcoin and Ether – provide good examples of digital assets that Director Hinman expressly posited no longer constitute securities primarily due to the decentralized nature of their use.[58] The "efforts of others" prong of the *Howey* Test requires that such efforts must be "undeniably significant ones, those essential managerial efforts which affect the failure or success of the enterprise."[59] Two seminal cases provide guidance on this prong for instruments traded in well-developed markets such as Bitcoin and Ether.[60] In both *Noa v. Key Futures* and *SEC v. Belmont Reid & Co*., the Ninth Circuit applied the *Howey* Test to the sale of precious metals, finding that the *Howey* Test is not satisfied if the expectation of economic return is based on market forces, and not on the efforts of an AP. Thus, the applicability of these cases to the analysis of Bitcoin and Ether within this prong of the *Howey* Test (and therefore the analysis of whether either Bitcoin or Ether is a security) depends on the existence of an established, decentralized market where the spot price is determined by ordinary market forces.

What is the role of the AP? Decentralized networks

As discussed above, the SEC's nascent regulatory framework for consumer tokens appears to be focused on a threshold question derived from the fourth prong of the *Howey* Test: Is the token-based network sufficiently decentralized/independent of the entrepreneurial efforts of the AP? There are several factors underlying this inquiry and each case requires careful analysis, and, without further guidance from the SEC, it is difficult to predict the appropriate weighting of such factors.

(a) Ongoing development and maintenance of the network

For a token-based network to be truly decentralized, no AP should have the ability to significantly and directly influence the value of the consumer tokens exchanged on the network. This implicitly includes ongoing efforts to develop and maintain the network. The Framework states it is more likely that a token purchaser is relying on the efforts of others if "[a]n AP is responsible for the development, improvement (or enhancement), operation, or promotion of the network, particularly if purchasers of the digital asset expect an AP to be performing or overseeing tasks that are necessary for the network or digital asset to achieve or retain its intended purpose or functionality." Open-source projects, where a variety of parties may contribute to the ongoing development of the network, clearly have a greater chance of meeting this requirement.

(b) Use of token sale proceeds

Similarly, the expected use of proceeds from a related token sale can impact whether a related token-based network is sufficiently decentralized. For example, a use of proceeds that involves further development and maintenance of the network could lead to a conclusion that the efforts of the issuer remain central to the value of the token. The Framework states that reasonable expectation of profit is more likely to be present if "[t]he AP continues to expend funds from proceeds or operations to enhance the functionality or value of the network or digital asset." This further supports the use of traditional financing instruments, coupled with economic rights in future token offerings. Issuers utilizing such instruments would be able to fund the development of their network from the investments received pursuant to such instruments and would, subsequently, be able to use the proceeds from token sales to deliver a return of

capital to investors, thereby clearly distinguishing early-stage investments from token purchases and supporting the position that the tokens themselves should not be deemed to be securities.

(c) Network governance

The Framework also indicated that a token-based network's governance structure will be considered when determining whether such network is decentralized.[61] In its most simple form, a decentralized governance structure would provide token holders the ability to directly determine matters relevant to the network's development. Reliance on the efforts of others is more likely to be deemed present if an AP has a continuing managerial role in network governance, including exercising judgment concerning the network or the characteristics and rights that the digital asset represents. The sufficient decentralization argument is strengthened if the AP can avoid playing a lead role in making decisions regarding governance issues, code and protocol updates, and how third parties participate in the validation of transactions that occur with respect to the digital asset.

(d) Robust token economy

The value of tokens on certain token-based networks is driven by a robust token economy pitting a number of different forces with different operating incentives against each other. These competing elements will be ascendant, and have a corresponding impact on the token value, at differing times. Courts have reasoned that this sort of market valuation mechanism is critical to distinguish a commodity from a security, as the value in the instrument is created by these broad market forces rather than the efforts of others.[62] The Framework also recognizes this principle, noting that token "[p]rice appreciation resulting solely from external market forces impacting the supply and demand for an underlying asset generally is not considered "profit" under the *Howey* test." Filecoin[63] is an apt example of a robust economic structure that helps ensure market forces drive token values independent of the AP's efforts. The Filecoin network involves three network participants: (i) clients, who pay to store and retrieve data; (ii) storage miners, who provide data storage to the network; and (iii) retrieval miners, who provide data retrieval to the network.[64] As a result, the competing activities of these three groups create the value of a Filecoin token through the creation of supply and demand economics. This also means the success of the Filecoin network hinges upon a sufficient number of market participants contributing to the network simultaneously, which is a premise reflected in the high proportion of Filecoin tokens allocated to miners in exchange for storage and retrieval services.[65]

There are numerous token-based networks and token economy models that similarly promote the development of a robust economic structure. The success of most decentralized token-based marketplaces, whether for data storage, digital assets in virtual worlds, artificial intelligence, real estate or intellectual property, is dependent on market participants driving the value of the networks and its corresponding tokens. As a result, these marketplaces, like those for Bitcoin and Ether (which rely on market participants to record transactions on their respective blockchains), have a market valuation mechanism that is helpful in distinguishing a commodity from a security.

Is the asset designed for consumptive purposes? Consumer tokens and consumer token sales

Numerous consumer token and consumer token sale features warrant consideration in furthering the consumer token analysis to determine whether the securities laws may apply.

(a) Functioning network

A factor closely related to the role of the AP, though distinct, is the question of whether the token-based network is "fully functioning or in the early stages of development."[66]

A common feature of many early token sales was that they were commenced before the consumer could actually utilize the token. While some consumer goods are purchased in this manner (*e.g.*, concert tickets or a new Tesla car), consumer token presales complicate the analysis of whether "the primary motivation for purchasing the digital asset is for personal use or consumption."[67] Although it remains difficult to assign weighting to the factors presented in the Framework, network functionality appears to be a factor that has significant bearing. As such, issuers should, to the extent possible, launch their token-based network prior to initiating consumer token sales.

(b) Secondary markets and transferability

In February 2018, then SEC Chairman Jay Clayton testified before the US Senate Committee on Banking, Housing, and Urban Affairs, in part sharing his particular concern for token issuers and emphasizing the secondary market trading potential of the tokens offered for sale.[68] This line of thinking clearly follows the *Gary Plastic* case, where the marketing of a non-security investment (*i.e.*, bank certificates of deposit) that included the promise of a secondary market transmutes the certificates of deposit into investment contracts.[69] Accordingly, the Framework states that if the AP promises to arrange trading of the digital asset on a secondary market, this means the token purchasers reasonably rely on the AP for liquidity, strongly supporting the view that such token is a security. However, the mere availability of a secondary market developing following a token sale arguably should not be dispositive and, perhaps, should not matter at all. Again, *Gary Plastic* stands for the notion that it is the *marketing* of the "investment" based on the potential of the secondary market that is what makes the instrument a security. Of course, there are many everyday commodities for which secondary markets regularly develop – in fact, eBay has built a robust business on this basis – and the mere existence of such markets does not transmute the instruments into securities.

For example, a large number of active market participants is critical to the success of Filecoin's network. It is difficult to imagine a scenario where it could achieve the critical mass of network participants necessary if such network participants were restricted from exchanging in some way their Filecoin tokens with other participants for other digital assets or tokens as part of continually broadening the universe of token holders. In order for a network to work under isolated conditions, where such transfers were not permitted, not only would suppliers have to consume the resources created by the network, but maintaining a balance among suppliers and producers would be exceedingly difficult. The secondary market transactions accordingly act to balance the various economic demands without any one actor having to play all roles. Otherwise, for Filecoin, a miner would need to both provide and consume storage and retrieval services, because consumption would be the only way to realize the economic gain in exchange for providing such services. As a result, there would be little incentive for the miner to participate on such a network. A similar case can be made for any network that includes both suppliers/producers of goods or services and consumers of goods or services. Furthermore, supply on any such market would decrease rapidly if the inputs required to produce the supply of goods and services were not principally derived from the tokens received upon sale, or if an insufficient number of other goods and services were available to enable suppliers to consume all of the tokens they earn within such marketplace. Given the negative effect on network participation that limiting secondary market activity would have, it is likely that overly broad restrictions would impede competition and that only the largest and most-established marketplaces would succeed.

Because of the foregoing, a measured approach to addressing secondary market activity and transferability is advisable. Fortunately, the flexibility arising out of ongoing innovation in blockchain technology provides companies with several options. First, purchasers of consumer tokens in a consumer token sale could be required to agree to a lockup mechanism, whereby a smart contract prevents the purchaser from selling their tokens for a certain period of time or until they participate on the network in the required manner. The purchaser's tokens could be unlocked initially only in the event they were utilized on the platform itself first, and thereafter could be traded in the secondary market. Second, a tiered transfer fee or other incentive structure could be implemented, whereby the fees (or other similar incentives) for tokens transferred in connection with participation on the token-based network could be lower than the fees for transfers to non-network participants. In each of these cases, initial purchasers would not have the same profit motive in seeking secondary market for token sales as they may have in a typical token offering.

Director Hinman appears to have suggested as much in his enumerated factors.[70]

(c) Inflationary issuances

Another aspect of consumer token sale structures that warrants discussion is the impact of inflationary/deflationary pressures in token economies. Depending on the token structure, there are a number of scenarios in which subsequent issuances of tokens in exchange for contributions to the economy of the network can simultaneously facilitate network growth while limiting the immediate speculative potential of the token. For example, Filecoin's token allocation design made 70% of the total Filecoin tokens available for miners in exchange for data storage and retrieval services. As those tokens will be subsequently distributed and "earned" by miners, the Filecoin token purchasers are "diluted" in an inflationary sense. However, unlike in the context of an equity security where dilution is significant because the valuation of the interest is always proportionate to the relative interest in the enterprise value, here the value of the token is based on the value of the goods and services that may be received in exchange, and the market supply and demand for such goods and services. Thus, the impact of dilution on a true consumer token is quite different and the value of the token should correspond more directly to the value to the consumer of the applicable goods and services. As a result, consideration should be given to the supply dynamics of a token economy.[71] Ultimate control over dilutive issuances is also a factor in network governance, which may impact the analysis above regarding the decentralization of a given network.

(d) Token retention

To date, a common feature of token offerings has been the retention of the tokens by issuers for distribution to founders, employees, advisors and investors. In instances where there are reasonable and justifiable grounds to believe that these individuals can and will consume these tokens through their own market participation and will thus assist in the seeding of the network, then consumer token issuers should not be dissuaded from including the retention of consumer tokens in their allotment strategy. However, issuers should exercise caution in doing so, particularly in cases where the products and services offered on an issuer's network or the number of tokens retained could not reasonably be consumed by its founders, employees, advisors and investors. In such instances, it would be difficult to make a credible argument to the SEC that such tokens are not being held for investment purposes.[72] The Framework states that token retention by an AP cuts towards reliance on the efforts of others given that token "[p]urchasers would reasonably expect the AP to undertake efforts to promote its own

interests" by taking actions that enhance the value of the digital asset. In addition, such retention of tokens also makes it more difficult for the token issuer to demonstrate that the tokens are "[d]ispersed across a diverse user base[,]" rather than being "[c]oncentrated in the hands of a few that can exert influence[.]"[73]

As a result, companies who wish to reward their teams for the successful development of a token-based network giving rise to a consumer token sale should look to traditional equity compensation methods, which can be augmented by consumer tokens to the extent a viable use case can be established. Additionally, selling restrictions with respect to both timing and price of tokens by such holders could be adopted to bolster the argument that such grants were not made to persons with an investment intent.

(e) Virtual currency peg/stablecoins

Another means of limiting the speculative potential in the purchase and sale of consumer tokens could be the adoption of token structures that initially peg the value of the consumer token to fiat or virtual currency, also known as a "stablecoin." The Framework highlights that tokens designed and marketed as virtual currencies are less likely to be considered securities under the *Howey* Test if the token can be used to pay for goods or services without first having to convert it to fiat currency or another token. In addition, the token must operate as a store of value that can be saved, retrieved, and exchanged for something of value at a later time. In the Turnkey Jet matter, the company alerted the SEC of its intent to issue "tokenized jet cards" (tokens) on a user platform facilitating the procurement of chartered airline flights. In its letter to the SEC, Turnkey Jet made clear that consumers of these tokens would be "motivated . . . by a desire to obtain on-demand air charter services," not by an expectation of future profits. Accordingly, Turnkey Jet maintained that these tokens would not be securities under the *Howey* framework. The SEC agreed, and identified several key attributes of the Turnkey Jet tokens that highlighted their consumptive utility and non-speculative nature. Specifically, the Turnkey Letter noted that Turnkey Jet's tokens would be immediately usable, have a fixed value of one USD per token and would be marketed in a manner that emphasized their functionality and not the potential for an increase in their market value. Similarly, in issuing the PoQ Letter, the SEC noted that PoQ's token having a fixed price factored into its considerations.[74]

As an alternative, in the case of an early-stage marketplace, an issuer could incentivize sellers to advertise their products or services in both the network's native virtual currency/token, as well as, for example, Ether, with the price of the goods or services being determined by the market price of Ether. The transaction could then be consummated in the native token of the network. This structure could have the effect of deterring speculative purchases at the time of an issuer's consumer token sale because the price of the token would presumably face downward pressure to remain in line with the exchange rate with the virtual currency peg. As a result, a virtual currency peg could result in the price of a given consumer token being primarily influenced by individuals or events beyond the token issuer's control and may therefore be viewed favorably by the SEC.[75] Once a larger and more functional network was operational with APs, these incentivizing schemes could be removed to allow for free market activity.

We would note that stablecoins may be swaps subject to CFTC regulation. Such structure would need to be carefully considered under commodities laws.

(f) Token sale legal documentation

Another means of discouraging purchasers of consumer tokens from an expectation of profit could be found in the documentation used in sales of tokens by issuers. Such

agreements could include representations and warranties requiring purchasers to state that their intention is to use such consumer tokens on the issuer's network. As discussed above, such documentation could also include lockup mechanisms, whereby the purchaser's tokens could be "locked" using a smart contract for a specified period. Furthermore, instruments could grant issuers first refusal with respect to any purchaser's tokens, whereby the issuer would be entitled to repurchase the tokens held by a user if the user had determined not to use them on the issuer's network. In many respects, this could be functionally similar to rights of return that are commonly provided by retailers with respect to tangible consumer goods, and issuers may be well advised to allocate a small percentage of any consumer token sales for such repurchases. While on most networks the issuer will only ever have privity of contract with the initial purchasers of consumer tokens, utilization of these mechanisms could substantially reduce the risk of such purchasers having an expectation of requiring the protection of securities laws. However, establishment of valuation protocols and resale price, as well as the potential of a withdrawal of cash from an issuer, may detract from the attractiveness of this alternative.

Seeding network activity and achieving decentralization

Based on the foregoing considerations, issuers who both operate decentralized networks featuring tokens designed for consumption, and sell such tokens in a manner designed to dissuade purchases for investment, should be capable of avoiding the application of securities laws to such token sales under the *Howey* Test. However, this current paradigm appears to create a paradox, given that the process of creating a decentralized and functional network on which consumer tokens can be utilized necessitates that issuers first seed network activity by issuing consumer tokens in transactions that do not trigger the application of the securities laws.

As a result, issuers may seek to seed their network through the distribution of consumer tokens via "airdrops" and other distributions to affiliates, vendors and community members. Such distributions promote network activity, facilitate the implementation of governance procedures and enable network testing prior to full launch. The information garnered from this process enables developers to resolve potential issues and simultaneously enhances the credibility of the project both within and outside its community. Furthermore, such activity can help consumers better understand the value of the overall network and each consumer token, which ultimately promotes market efficiency. The benefits of such seed activity extend to consumer token issuances targeting strategic partners, who may also assist with the development of the network prior to launch. In addition, this seed activity permits the nascent token economy of the platform to grow, allowing forces beyond those of the initial AP to begin to determine the value of the token. As a result, this activity directly addresses several of the factors identified by Director Hinman and can strengthen the case that a particular token is a consumer token.[76]

Nonetheless, issuers need to be aware that the SEC takes the view that the securities laws apply to airdrops of tokens, even though no money or digital currency funds are given by airdrop recipients. For example, in the early days of the internet, some issuers sought to issue free shares of common stock to registered website users, as part of a broader promotion to attract traffic to the website and promote brand awareness and loyalty. The SEC took the view that the free distribution of shares was a "sale" of securities.[77] Similarly, the SEC has taken the view that the spin-off of shares of a subsidiary as a free stock dividend to an

issuer's shareholders can be a sale of securities.[78] As a result, unless and until the SEC gives more lenient guidance, airdrops should be considered and conducted in the same manner as token offerings, generally, as discussed above.

Although sufficient decentralization is difficult to define precisely, there are potential steps that the SEC can take to provide market participants with greater clarity. The SEC has highlighted a number of factors to consider when inquiring whether a token-based network is sufficiently decentralized. Of course, as noted by Commissioner Peirce,[79] it would be helpful if the SEC could provide clarity as to the appropriate weighting of such factors. One of the primary goals of securities law is to protect investors through the mitigation of information asymmetries that exist between issuers and investors. We propose that this principle should inform the weighting of the factors used to measure the sufficient decentralization of a network. As a result, there should be less emphasis on factors that penalize tokens simply because they bear similarity to securities in their marketing, and greater emphasis on factors that have a clear nexus to the reduction of information asymmetries. For example, the decentralization of network development and maintenance as well as network governance should be factors that are amongst the most heavily weighted. If such activity is truly decentralized, the less likely it is for there to be information asymmetries between network users and a powerful central group that manages the network.

On the other hand, the SEC should give less weight to factors such as a token's transferability or the existence of secondary markets for it. As discussed, a commodity does not become a security simply because there are secondary markets on which it is traded. It is critical to the success of certain token-based networks to have a large number of active market participants. If users on such networks were restricted from exchanging in some way their tokens with other potential participants, it is unlikely that the network could reach the necessary critical mass.

Furthermore, the SEC should provide clear guidance regarding potential pathways for achieving sufficient decentralization. Under the current regulatory framework, developers need to be wary that the seeding of their network via token "airdrops" and other distributions to affiliates, strategic partners, vendors and community members could be deemed to be a securities offering given that the issuer may receive a direct benefit from such distributions. However, these parties are unlikely to require protection from the information asymmetries securities laws are designed to guard against and these distributions are a vital step for many networks to be able to achieve decentralization. Such distributions often promote network activity, facilitate the implementation of governance procedures, enable network testing prior to full launch and incentivize third-party development work. In addition, this seed activity permits the nascent token economy of a network to grow, allowing forces beyond those of the initial promoter to begin to determine the network's value. As a result, this activity directly addresses several of the factors identified in the Framework and can strengthen the case that a particular network is decentralized.

New SEC Chairman may mean new rules for crypto

On August 3, 2021, Gary Gensler, the newly appointed Chairman of the SEC, gave a speech[80] on the digital asset industry. The speech offered some indication of what he expects the SEC to focus on in this area but did not provide concrete guidance for industry participants looking for clarity on regulatory uncertainties. He did, however, make clear that he believes "we just don't have enough investor protection in crypto" and that the SEC will play a more active role in regulating the industry. Mr. Gensler, therefore, is particularly focused on the investor protection pillar of the SEC's mission.

In his speech, he took a broad view of the securities laws and spoke of digital asset innovation primarily through the lens of consumer and market protection. Mr. Gensler was also clear that he believes the mandate of the SEC and other regulators is far-reaching, asserting that "we have taken and will continue to take our authorities as far as they go." According to Mr. Gensler, the *Howey* Test is only one of the ways the SEC determines whether a digital asset must comply with the securities laws.

Mr. Gensler also echoed former SEC Chairman Jay Clayton's views when Mr. Clayton testified in 2018 that "to the extent that digital assets like [initial coin offerings, or ICOs] are securities—and I believe every ICO I have seen is a security—we have jurisdiction, and our federal securities laws apply." Whether this view includes more modern iterations of token distributions that do not include a public sale remains to be seen.

Conclusion

Much has been made of the need for certainty, and perhaps even innovation, in the application of various laws, including the US securities and commodities laws, to commercial activities relating to blockchain, cryptocurrencies and related technologies. After all, the applicable federal securities statute is over 85 years old, and the seminal case, *Howey*, is more than 70 years old. While age is not in itself sufficient to discount governing law (after all, the US Constitution is now over 230 years old), digital assets present unique questions that our current laws do not always appear equipped to answer. That said, the SEC has not retreated from the application of existing precedent when examining token transactions. Nevertheless, given the underlying principles, and the SEC's public statements, there is some reason for optimism that the existing framework will permit at least some transactions in tokens to be executed without the application of the federal securities laws. We suggest, however, that it continues to be prudent for interested parties to seek guidance directly from the SEC staff before proceeding.

* * *

Endnotes

1. Robert Stevens, *SEC Faces Stiff Test in Regulating DeFi, Says Hester Peirce*, Decrypt (Sept. 4, 2020), https://decrypt.co/40819/sec-faces-stiff-test-regulating-defi-says-hester-peirce.
2. The Digital Asset Taxonomy published by ConsenSys, a leader in the blockchain field, defined "consumer tokens" as "inherently consumptive in nature, which means that their intrinsic features and primary use are to represent, or facilitate the exchange of or access to, a limited set of goods, services, or content. The term "consumer" here refers to the consumptive nature of the relevant goods, services, or content, which businesses as well as individual users may ultimately use or consume[.]" DIGITAL ASSET TAXONOMY: FROM THE PERSPECTIVE OF GLOBAL FRAMEWORKS FOR SECURITIES AND FINANCIAL INSTRUMENTS, https://thebkp.com/token-taxonomy/ (last visited July 26, 2018).
3. *SEC v. W.J. Howey Co.*, 328 U.S. 293 (1946).
4. 15 U.S.C. §§ 77b(a)(1), 78c(a)(10).
5. *See Howey* at 301.
6. *See id.*

7. *See* Latham & Watkins, SEC Takes Enforcement Action against Utility Token ICO, Client Alert No. 2257 (Dec. 20, 2017), https://www.lw.com/thoughtLeadership/SEC-vigorously-police-utility-token-ICO.
8. *Gary Plastic Packaging v. Merrill Lynch, Pierce, Fenner & Smith Inc.*, 756 F.2d 230 (2d Cir. 1985).
9. SEC, Framework for "Investment Contract" Analysis of Digital Assets (2019), https://www.sec.gov/corpfin/framework-investment-contract-analysis-digital-assets.
10. TurnKey Jet, Inc., SEC No-Action Letter (Apr. 3, 2019), https://www.sec.gov/divisions/corpfin/cf-noaction/2019/turnkey-jet-040219-2a1.htm; Pocketful of Quarters, Inc., SEC No-Action Letter (July 25, 2019), https://www.sec.gov/corpfin/pocketful-quarters-inc-072519-2a1.
11. *SEC v. Kik Interactive Inc.*, No. 19-cv-5244 (S.D.N.Y. filed June 4, 2019).
12. *Id.*
13. *Kik Responds to SEC Complaint*, PR Newswire (June 4, 2019), https://www.prnewswire.com/news-releases/kik-responds-to-sec-complaint-300862114.html [hereinafter Kik Response Article].
14. Wells Submission of Kik Interactive Inc. and the Kin Ecosystem Foundation at 17 (Dec. 10. 2018), https://www.kin.org/wells_response.pdf.
15. Kik Response Article.
16. *Telegram to Return $1.2 Billion to Investors and Pay $18.5 Million Penalty to Settle SEC Charges*, Sec. & Exch. Comm'n (June 26, 2020), https://www.sec.gov/news/press-release/2020-146; *SEC v. Telegram Group Inc.*, No. 19 Civ. 9439 (PKC) (S.D.N.Y. filed Mar. 20, 2020).
17. *SEC v. Kik Interactive Inc.*, No. 19-cv-5244 (S.D.N.Y. filed June 4, 2019); *SEC v. Telegram Group Inc.*, No. 19 Civ. 9439 (PKC) (S.D.N.Y. filed Mar. 20, 2020).
18. *SEC v. Telegram Group Inc.*, No. 19 Civ. 9439 (PKC) at 2 (S.D.N.Y. filed Mar. 20, 2020).
19. *See* Hester M. Peirce, Running on Empty: A Proposal to Fill the Gap Between Regulation and Decentralization (Feb. 6, 2020), https://www.sec.gov/news/speech/peirce-remarks-blockress-2020-02-06.
20. *See* Hester M. Peirce, Commissioner, Sec. & Exch. Comm'n, Token Safe Harbor Proposal 2.0 (Apr. 13, 2021), https://www.sec.gov/news/public-statement/peirce-statement-token-safe-harbor-proposal-2.0?utm_medium=email&utm_source=govdelivery.
21. *See* Joint Staff Statement on Broker-Dealer Custody of Digital Asset Securities (July 8, 2019), https://www.sec.gov/news/public-statement/joint-staff-statement-broker-dealer-custody-digital-asset-securities.
22. *See* Custody of Digital Asset Securities by Special Purpose Broker-Dealers (Dec. 23, 2020), https://www.sec.gov/rules/policy/2020/34-90788.pdf.
23. *See*, *e.g.*, 7 U.S.C. §§ 6c(a), 9, 12(a)(5), 15; 17 C.F.R. § 180.1; *see also* Prohibition on the Employment, or Attempted Employment, of Manipulative and Deceptive Devices and Prohibition on Price Manipulation, 76 Fed. Reg. 41398 (July 14, 2011), https://www.gpo.gov/fdsys/pkg/FR-2011-07-14/pdf/2011-17549.pdf; Statement of Commissioner Dawn D. Stump on the CFTC's Regulatory Authority Applicable to Digital Assets (Aug. 23, 2021), https://www.cftc.gov/PressRoom/SpeechesTestimony/stumpstatement082321?utm_source=govdelivery.
24. Timothy Massad, Chairman, Commodity Futures Trading Comm'n, Testimony of Chairman Timothy Massad before the US Senate Committee on Agriculture, Nutrition, and Forestry (Dec. 10, 2014), http://www.cftc.gov/PressRoom/SpeechesTestimony/opamassad-6 [hereinafter 2014 Massad Senate Testimony].

25. During this time, the CFTC has settled enforcement actions with exchanges, stressing a distinct aspect of its jurisdictional oversight in each: from establishing that virtual currencies are "commodities," to applying the retail commodity rules to leveraged virtual currency transactions, to asserting jurisdiction over virtual currency derivatives. *See* Latham & Watkins, CFTC Brings Significant Enforcement Action Against Online Cryptocurrency Exchange, Client Alert No. 1980 (June 20, 2016), https://www.lw.com/thoughtLeadership/CFTC-brings-significant-enforcement-action-against-online-cryptocurrency-exchange; Latham & Watkins, Enforcement Trends in Cryptocurrency, Client Alert No. 1904 (Dec. 9, 2015), https://www.lw.com/thoughtLeadership/lw-enforcement-trends-cryptocurrency; Latham & Watkins, Cryptocurrencies Are Commodities: CFTC's First Bitcoin Enforcement Action, Client Alert No. 1874 (Sept. 21, 2015), https://www.lw.com/thoughtLeadership/LW-CFTC-first-bitcoin-enforcement-action.
26. *See*, *e.g.*, CFTC Release PR7938-19, CFTC Charges Company and its Principal in $147 Million Fraudulent Bitcoin Trading Scheme (June 18, 2019), https://www.cftc.gov/PressRoom/PressReleases/7938-19; CFTC Release PR7839-18, CFTC Orders Former Virtual Currency Trader to Pay More than $1.1 Million for Fraudulent Bitcoin and Litecoin Scheme (Nov. 9, 2018), https://www.cftc.gov/PressRoom/PressReleases/7839-18; CFTC Release PR7813-18, CFTC Charges Two Defendants with Fraudulent Solicitation, Impersonation of a CFTC Investigator, and Forging CFTC Documents, All in Attempt to Steal Bitcoin (Sept. 28, 2018), https://www.cftc.gov/PressRoom/PressReleases/7813-18; CFTC Release PR7714-18, CFTC Charges Multiple Individuals and Companies with Operating a Fraudulent Scheme Involving Binary Options and a Virtual Currency Known as ATM Coin (Apr. 18, 2018), https://www.cftc.gov/PressRoom/PressReleases/7714-18; CFTC Release PR7614-17, CFTC Charges Nicholas Gelfman and Gelfman Blueprint, Inc. with Fraudulent Solicitation, Misappropriation, and Issuing False Account Statements in Bitcoin Ponzi Scheme (Sept. 21, 2017), http://www.cftc.gov/PressRoom/PressReleases/pr7614-17.
27. Retail Commodity Transactions Involving Certain Digital Assets, 85 Fed. Reg. 37,734 (June 24, 2020), https://www.govinfo.gov/content/pkg/FR-2020-06-24/pdf/2020-11827.pdf.
28. *See* Accepting Virtual Currencies from Customers into Segregation (Oct. 21, 2021), https://www.cftc.gov/csl/20-34/download.
29. The following discussion of consumer token presales only seeks to address fundraising instruments utilized for pure consumer token issuances and not instruments utilized for pure security token issuances, which often have similar terms. We note that the presale of a token designed to be a security is a far easier analysis, as each of the instruments should be offered and sold in compliance with securities law requirements and ordinary corporate finance practices.
30. *See*, *e.g.*, Juan Batiz-Benet, Jesse Clayburgh & Marco Santori, THE SAFT PROJECT: TOWARD A COMPLIANT TOKEN SALE FRAMEWORK (Oct. 2, 2017), https://saftproject.com/static/SAFT-Project-Whitepaper.pdf [hereinafter SAFT Whitepaper].
31. In addition to the securities law issues and commodities law issues discussed below, the SAFT and similar presale instruments can raise tax concerns in light of the uncertainty regarding their treatment for US federal income tax purposes. It is possible that an issuer could be subject to US federal income tax on proceeds from SAFT sales on a current basis, particularly where the underlying tokens are consumer tokens.
32. *Id.* (Section 5(c) of the SAFT, which is included as Exhibit 1 to the SAFT Whitepaper): "(c) The Purchaser has no intent to use or consume any or all Tokens on the corresponding

blockchain network for the Tokens after Network Launch. The Purchaser enters into this security instrument purely to realise profits that accrue from purchasing Tokens at the Discount Price."

33. Defined in the SAFT as "a *bona fide* transaction or series of transactions, pursuant to which the [issuer] will sell the Tokens to the general public in a publicized product launch." Simple Agreement for Future Tokens, https://saftproject.com/static/Form-of-SAFT-for-token-pre-sale.docx (last visited July 29, 2018).
34. We note that some practitioners have proposed that if the network launch occurs more than six months after the SAFT sale, they should constitute two distinct plans of financing and thus would not be integrated in accordance with the safe harbor of Rule 502 under the Securities Act. In this regard, we would consider the concurrent settlement to negate this proposition. Similarly, the SAFT itself may constitute an offering of the underlying token that is continuous until delivery. In any event, we would expect that the tokens received by SAFT investors would nevertheless constitute securities on the date of delivery given the nature of the SAFT offering and the delivery of tokens to investors, unless the network has become sufficiently decentralized in the interim such that the "efforts" prong of the *Howey* Test was no longer satisfied.
35. *See SEC v. Kik Interactive Inc.*, No. 19-cv-5244 (S.D.N.Y. filed June 4, 2019).; *SEC v. Telegram Group Inc.*, No. 19 Civ. 9439 (PKC) (S.D.N.Y. filed Mar. 20, 2020).
36. *SEC v. Kik Interactive Inc.*, No. 19-cv-5244 (S.D.N.Y. filed June 4, 2019).
37. *SEC v. Telegram Group Inc.*, No. 19 Civ. 9439 (PKC) at 43 (S.D.N.Y. filed Mar. 20, 2020).
38. *See*, *e.g.*, 2014 Massad Senate Testimony.
39. *See* 7 U.S.C. § 1a(47)(A)(ii) ("the term 'swap' means any agreement, contract, or transaction . . . that provides for any purchase, sale, payment, or delivery . . . that is dependent on the occurrence, nonoccurrence, or the extent of the occurrence of an event or contingency associated with a potential financial, economic, or commercial consequence"). Swap contracts are subject to a myriad of CFTC regulations under the CEA, as amended by the Dodd-Frank Wall Street Reform and Consumer Protection Act of 2010 (the Dodd-Frank Act), including the requirement that over-the-counter (OTC) swap counterparties be "eligible contract participants." *Id.* § 1a(18) (defining eligible contract participants (ECPs)). An individual can only qualify as an ECP if such person has amounts invested on a discretionary basis, the aggregate of which is in excess of $10 million; or $5 million and enters into swaps in order to manage the risk associated with an asset owned or liability incurred (or reasonably likely to be owned or incurred) by such person. *Id*. § 1a(18)(A)(xi). If one or both of the parties to a swap transaction are non-ECPs, the swap must be executed on a CFTC-registered designated contract market. *Id*. § 2(e).
40. Both the CEA and CFTC regulations thereunder have long recognized a forward contract exclusion from futures contracts. *See* 7 U.S.C. § 1a(27) ("The term 'future delivery' does not include any sale of any cash commodity for deferred shipment or delivery."). Following enactment of the Dodd-Frank Act in 2010, the sale of a non-financial commodity for deferred shipment or delivery was also excluded from the definition of "swap" in Section 1a(47) of the CEA under the Non-Financial Forward Contract Exclusion. *Id.* § 1a(47)(B)(ii).
41. 17 C.F.R. § 34.3(a).
42. Both the CEA and CFTC regulations thereunder have long recognized a forward contract exclusion from futures contracts. *See* 7 U.S.C. § 1a(27) ("The term 'future delivery' does not include any sale of any cash commodity for deferred shipment or

delivery."). Following enactment of the Dodd-Frank Act in 2010, the sale of a non-financial commodity for deferred shipment or delivery was also excluded from the definition of "swap" in Section 1a(47) of the CEA under the Non-Financial Forward Contract Exclusion. *Id.* § 1a(47)(B)(ii).

43. *See* Further Definition of "Swap," "Security-Based Swap," and "Security-Based Swap Agreement;" Mixed Swaps; Security-Based Swap Agreement Recordkeeping, 77 Fed. Reg. 48208, 48228 (Aug. 13, 2012), https://www.gpo.gov/fdsys/pkg/FR-2012-08-13/pdf/2012-18003.pdf [hereinafter Products Release].
44. As the CFTC has noted, "the underlying postulate of the [forward] exclusion is that the [CEA's] regulatory scheme for futures trading simply should not apply to private commercial merchandising transactions which create enforceable obligations to deliver but in which delivery is deferred for reasons of commercial convenience or necessity." *Id.* at 48228.
45. The CFTC drew a clear distinction between commercial market participants and investors in the Products Release, stating that "[a] hedge fund's investment activity is not commercial activity within the CFTC's longstanding view of the Brent Interpretation." *Id.* at 48229. The "Brent Interpretation" refers to the CFTC's 1990 interpretation of the application of the forward contract exclusion from the definition of "future delivery" in the context of "book-outs" transactions, which the CFTC extended in the Products Release to apply to the forward contract exclusion from the swap definition for non-financial commodities. Statutory Interpretation Concerning Forward Transactions, 55 Fed. Reg. 39188 (Sept. 25, 1990), https://cdn.loc.gov/service/ll/fedreg/fr055/fr055186/fr055186.pdf.

    Moreover, the CFTC continued to elaborate on its discerning view of "commercial" in the Products Release, stating that "an investment vehicle taking delivery of gold as part of its investment strategy would not be engaging in a commercial activity within the meaning of the Brent Interpretation." Products Release at 48229. However, if the investment vehicle were to own a chain of jewelry stores and would purchase gold on a forward basis to provide raw materials for the jewelry store, the CFTC would consider such activity to fall within the forward contract exclusion under the Brent Interpretation. *Id*. Notably, the CFTC stated in the Products Release that, for purposes of the "swap" definition, the Non-Financial Forward Contract Exclusion will be interpreted in a manner consistent with the CFTC's historical interpretation of the existing forward exclusion with respect to futures. As a result, the Brent Interpretation analysis is applicable for purposes of evaluating the Non-Financial Forward Contract Exclusion as it pertains to the "swap" definition. *Id*. at 48227–48228.
46. *See id.*; *supra* text accompanying note 16.
47. 7 U.S.C. § 1a(47)(A)(i) ("the term 'swap' means any agreement, contract, or transaction . . . that is a put, call, cap, floor, collar, or similar option of any kind that is for the purchase or sale, or based on the value, of 1 or more . . . commodities").
48. *See* 17 C.F.R. § 32.3(c).
49. *See* 17 C.F.R. § 32.3(a).
50. Under Section 2(f) of the CEA, a hybrid instrument is "predominantly a security" and exempt from the provisions of the CEA if:
    1. the hybrid instrument issuer receives payment in full of the hybrid instrument's purchase price, substantially contemporaneously with delivery of the hybrid instrument;

2. the hybrid instrument purchaser/holder is not required to make any payment to the issuer in addition to the purchase price described above, whether as margin, settlement payment or otherwise, during the life of the hybrid instrument or at maturity;
3. the hybrid instrument issuer is not subject by the instrument's terms to mark-to-market margining requirements; and
4. the hybrid instrument is not marketed as a contract of sale of a commodity for future delivery (or option on such a contract) subject to the CEA.

7 U.S.C. § 2(f)(2).

51. This discussion assumes that prongs (i)–(iii) of the Hybrid Instrument Exemption are met with respect to any such presale instrument. Any such presale instrument must meet all four prongs of the exemption.
52. *See supra* text accompanying note 29; 7 U.S.C. § 2(e).
53. Such securities offerings are almost exclusively accomplished through the use of an exemption from registration, such as in a private placement that is limited to participants who are "accredited investors," as defined in 17 C.F.R. § 230.501, either under the more traditional-style private placement of Regulation D, Rule 506(b), or the crowdfunding compatible, Regulation D, Rule 506(c). Issuers may also consider utilizing Regulation CF or Regulation A, which permit sales to non-accredited investors after making certain filings with the SEC. For additional information, *see* Latham & Watkins, SEC Adopts Final Crowdfunding Rules, Client Alert No. 1893 (Nov. 10, 2015), https://www.lw.com/thoughtLeadership/lw-sec-adopts-crowdfunding-rules; Stephen P. Wink and Brett M. Ackerman, Crowdfunding Under the SEC's New Rules, 49 REV. OF SEC. & COMMODITIES REG. 267 (Dec. 21, 2016), https://www.lw.com/thoughtLeadership/crowdfunding-SEC-new-rules-2016.
54. While issuers should be cautious when granting such rights, generally the enterprise and its investors are best served when their interests align. In consumer token sales, the parties share a direct interest in ensuring the offering or distribution complies with applicable securities and commodities laws. In addition, all participants should share a similar interest in the maturing of the market for token presales, as in the traditional venture capital space, to attract capital from investors that have yet to approach the sector due to regulatory risks.
55. A discussion of the types of structures that may so qualify and the nature of the availability of the possible exemptions is beyond the scope of this chapter.
56. *See* Latham & Watkins, Token Presale Agreements and the ConsenSys Automated Convertible Note (May 22, 2019), https://www.lw.com/thoughtLeadership/token-presale-agreements-consensys-automated-convertible-note.
57. *See* Hinman Speech; *see also* Latham & Watkins, A Path Forward for Consumer Tokens, Client Alert No. 2336 (June 27, 2018), https://www.lw.com/thought Leadership/lw-a-path-forward-for-consumer-tokens.
58. *See* Hinman Speech.
59. *SEC v. Glenn W. Turner Enterprises Inc*., 474 F.2d 476, 482 (9th Cir. 1973) ("[T]he fact that the investors here were required to exert some efforts if a return were to be achieved should not automatically preclude a finding that the Plan or Adventure is an investment contract. To do so would not serve the purpose of the legislation. Rather we adopt a more realistic test, whether the efforts made by those other than the investor are the undeniably significant ones, those essential managerial efforts which affect the failure or success of the enterprise."); *see United Housing Found., Inc. v. Forman*, 421 U.S. 837, 855 (1975) (the "efforts of others" prong of the *Howey* Test requires that investors have a reasonable expectation of profit derived from the efforts of others).

60. In *Noa v. Key Futures, Inc*., the Ninth Circuit held that if the expectation of economic return from an instrument is based solely on market forces, and not on the efforts of a promoter, then the instrument does not satisfy this prong of the *Howey* Test. *Noa v. Key Futures, Inc*., 638 F.2d 77 (9th Cir. 1980). The scheme in *Noa* involved the sale of silver bars through high-pressure sales efforts, and the Ninth Circuit's decision rested primarily on the existence of a separate market for the instrument that the investor could sell into, such that the economic return was driven by the market price and not the efforts of the promoter: "Once the purchase of silver bars was made, the profits to the investor depended upon the fluctuations of the silver market, not the managerial efforts of Key Futures. The decision to buy or sell was made by the owner of the silver." *Id*. at 79.
SEC v. Belmont Reid & Co. involved a promoter that was involved in a gold mining operation who obtained prepayments from investors for the purchase of gold coins that would be obtained as a result of the mining operation. *SEC v. Belmont Reid & Co*., 794 F.2d 1388 (9th Cir. 1986). While the purchaser's return was highly dependent on the ability of the promoter to successfully mine and deliver the gold coins, the Ninth Circuit reasoned that the same non-performance risk exists in the context of any sale-of-goods contract in which the buyer pays in advance, and therefore that such a dependence on the promoter's efforts could not itself satisfy the *Howey* Test without making any such sale-of-goods contract a security. Instead, the Ninth Circuit held that the *Howey* Test was not satisfied in *Belmont Reid & Co*., because the purchasers who prepaid for the gold coins: "[H]ad as their primary purpose to profit from the anticipated increase in the world price of gold . . . In short, the purchaser[s] were speculating in the world gold market . . . To the extent the purchasers relied on the managerial skill of [the promoters] they did so as an ordinary buyer, having advanced the purchase price, relies on an ordinary seller." *Id.* at 1391.
61. *See id.*
62. *See supra* text accompanying note 46.
63. Please note that we have chosen Filecoin in this example in part because we have no connection to its activities.
64. Protocol Labs, FILECOIN: A DECENTRALIZED STORAGE NETWORK (Aug. 14, 2017), https://filecoin.io/filecoin.pdf.
65. CoinList, FILECOIN TOKEN SALE ECONOMICS, https://coinlist.co/assets/index/filecoin_index/Filecoin-Sale-Economics-e3f703f8cd5f644aecd7ae3860ce932064ce014dd60de115d67ff1e9047ffa8e.pdf (last visited July 26, 2018).
66. Hinman Speech; *see Munchee* Order; Jay Clayton, Chairman, Sec. & Exch. Comm'n, Statement on Cryptocurrencies and Initial Coin Offerings (Dec. 11, 2017), https://www.sec.gov/news/public-statement/statement-clayton-2017-12-11.
67. Hinman Speech.
68. Jay Clayton, Chairman, Sec. & Exch. Comm'n, Chairman's Testimony on Virtual Currencies: The Roles of the SEC and CFTC (Feb. 6, 2018), https://www.sec.gov/news/testimony/testimony-virtual-currencies-oversight-role-us-securities-and-exchange-commission. ("In short, prospective purchasers are being sold on the potential for tokens to increase in value with the ability to lock in those increases by reselling the tokens on a secondary market or to otherwise profit from the tokens based on the efforts of others. These are key hallmarks of a security and a securities offering.")
69. *See Gary Plastic* at 240–241.
70. *See* Hinman Speech ("Are the tokens distributed in ways to meet users' needs? For example, can the tokens be held or transferred only in amounts that correspond to a

purchaser's expected use? Are there built-in incentives that compel using the tokens promptly on the network, such as having the tokens degrade in value over time, or can the tokens be held for extended periods for investment?").

71. *See id.* ("Is token creation commensurate with meeting the needs of users or, rather, with feeding speculation?").
72. *See id.* ("Has this person or group retained a stake or other interest in the digital asset such that it would be motivated to expend efforts to cause an increase in value in the digital asset?").
73. *Id.*
74. Pocketful of Quarters, Inc., SEC No-Action Letter (July 25, 2019), https://www.sec.gov/corpfin/pocketful-quarters-inc-072519-2a1.
75. *See* Hinman Speech ("Are independent actors setting the price or is the promoter supporting the secondary market for the asset or otherwise influencing trading?").
76. *See id.* ("Are the assets dispersed across a diverse user base or concentrated in the hands of a few that can exert influence over the application?").
77. Simplystocks.com, SEC No-Action Letter (Feb. 4, 1999).
78. SEC Staff Legal Bulletin No. 4 (Sept. 16, 1997), https://www.sec.gov/interps/legal/slbcf4.txt.
79. Hester M. Peirce, How We Howey (May 9, 2019), https://www.sec.gov/news/speech/peirce-how-we-howey-050919.
80. *See* Gary Gensler, Chairman, Sec. & Exch. Comm'n, Remarks Before the Aspen Security Forum (Aug. 3, 2021), https://www.sec.gov/news/public-statement/gensler-aspen-security-forum-2021-08-03?utm_medium=email&utm_source=govdelivery.

* * *

Acknowledgments

The authors gratefully acknowledge the invaluable contributions to this chapter of Adam Bruce Fovent, Adam Zuckerman, and Deric Behar.

Yvette D. Valdez
Tel: +1 212 906 1797 / Email: yvette.valdez@lw.com

Yvette Valdez is a partner in the New York office of Latham & Watkins. Ms. Valdez is Co-Chair of the Commodities and Derivatives Regulation and Enforcement Practice, head of the US Derivatives Regulatory Practice, Co-Chair of the IBOR Transition Task Force, Co-Chair of the Global Blockchain & Cryptocurrency Task Force, and a member of the firm's Financial Institutions and Fintech Industry Groups and Financial Regulatory and Derivatives Practices. Ms. Valdez advises emerging companies, financial institutions, and investment managers on complex regulatory challenges in the development of bespoke financial crypto-asset and cryptocurrency technologies, including token sales, market infrastructure, trading, clearing, and settlement solutions on distributed ledger technology. She also advises clients on domestic and cross-border fintech initiatives in the derivatives markets. In addition, Ms. Valdez has significant experience representing dealers, intermediaries, and end-users in connection with derivatives (swaps and futures) legal and regulatory matters under the Dodd-Frank Act, the Commodity Exchange Act, as well as related CFTC, SEC, and prudential regulation.

Stephen P. Wink
Tel: +1 212 906 1229 / Email: stephen.wink@lw.com

Stephen Wink is a partner in the New York office of Latham & Watkins. Mr. Wink is a member of the Financial Regulatory Practice, Financial Institutions Group, Fintech Industry Group, and Co-Chair of the firm's Global Blockchain & Cryptocurrency Task Force. He advises a wide range of market players, including fintech companies, cryptocurrency issuers and platforms, investment banks, hedge funds, private equity firms, proprietary trading platforms, and other financial institutions. Mr. Wink has in-depth knowledge and broad experience advising institutions on regulatory and related matters, gained in part from a decade as general counsel of a full-service investment bank.

Paul M. Dudek
Tel: +1 202 637 2377 / Email: paul.dudek@lw.com

Paul Dudek is a partner in the Washington, D.C. office of Latham & Watkins. Mr. Dudek joined Latham after 23 years as Chief of the Office of International Corporate Finance in the US Securities and Exchange Commission's (SEC) Division of Corporation Finance. His practice covers all aspects of cross-border capital market transactions involving non-US companies and sovereigns, as well as related regulatory matters.

Latham & Watkins LLP

1271 Avenue of the Americas, New York, New York 10020, USA
Tel: +1 212 906 1200 / Fax: +1 212 751 4864 / URL: www.lw.com

An introduction to virtual currency money transmission regulation

Michelle Ann Gitlitz, Carlton Greene & Caroline Brown
Crowell & Moring LLP

Introduction

Virtual currencies allow individuals to effectuate fast, low-cost, seamless and secure cross-border transactions. For regulators, the proliferation of virtual currencies and these transactions has also increased potential money laundering, terrorism finance and consumer protection concerns. This chapter examines when businesses in the virtual currency arena may be obligated to comply with federal and state money transmission laws and regulations in the United States.

At the federal level, the Bank Secrecy Act (BSA)[1] requires banks, broker-dealers, money services businesses (MSBs) and many other types of financial institution to file certain reports (particularly suspicious activity reports or SARs), to preserve certain records, and to maintain anti-money laundering (AML) programs designed to prevent the institution from being used to facilitate financial crime. The Financial Crimes Enforcement Network (FinCEN) – a bureau of the U.S. Department of the Treasury – administers the BSA and is charged with protecting the U.S. financial system and combating money laundering and terrorism financing. FinCEN does this through the civil enforcement of BSA rules against regulated financial institutions, the promulgation of additional AML rules and guidance, and by maintaining a database of the reporting it receives from regulated financial institutions and other law enforcement information. FinCEN makes this information available to federal, state and local law enforcement agencies as well as financial regulators to aid their law enforcement missions. In addition, FinCEN produces its own analysis of the data to identify money laundering, terrorism financing, and other threats to the financial system and to make referrals to law enforcement. FinCEN is also the U.S. Financial Intelligence Unit (FIU), and cooperates with a network of more than 140 foreign FIUs to share information on such threats.[2] Many virtual currency businesses are regulated under the BSA as money transmitters, a form of MSB.

Separate from the federal regulations, nearly every U.S. state has its own laws governing money transmitters. There is some overlap in the design of these laws, but also many differences that require individualized consideration of each state. In many cases, these laws are vaguely drafted, or were designed in an era that did not contemplate virtual currency. Unlike federal AML rules, state money transmission laws are often not aimed at protecting against money laundering and terrorism financing. They focus instead on consumer protection, ensuring that a money transmitter will not lose, steal or misdirect the consumer's money.

The obligation of virtual currency businesses to consider not only federal law, but also a patchwork of varying state money transmitter statutes, has proven to be one of the greatest

regulatory challenges that virtual currency businesses face. The maze of state licensing regulations paired with FinCEN's federal requirements demand thoughtful consideration of legal compliance for any person or business that operates in the virtual currency industry.

Federal virtual currency money transmission

The BSA is a composite of multiple statutes, starting with the Currency and Financial Transactions Reporting Act of 1970 as amended by Title III of the USA PATRIOT Act of 2001 and other legislation.[3]

The BSA requires "financial institutions" to monitor their customers and their transactions and to identify and report suspicious activity to FinCEN in the form of SARs.[4] Financial institutions that encounter certain red flags of potential money laundering or terrorism financing associated with a customer or transaction are expected to investigate these indicators to determine whether a legitimate explanation for the activity can be found. If not, the institutions must file a SAR.[5] Periodically, FinCEN also publishes advisories and alerts providing additional red flags relating to specific industries or types of illicit activities. As an example, in July 2020, FinCEN published an alert providing red flags relating to a virtual currency scam involving the social media service Twitter, and asked convertible virtual currency (CVC) exchanges and other financial institutions to report similar suspicious transactions to FinCEN.

In addition to filing SARs and other reports with FinCEN, banks and broker-dealers are required to conduct customer due diligence to understand the nature and purpose of their customers' relationships with the institution and to operate customer identification programs, under which they must obtain and verify certain identifying information about their customers, such as full name, date of birth, address, and a taxpayer identification number (i.e., a Social Security number).[6] Money transmitters – as a form of MSB – are subject to slightly different requirements: they do not have a categorical obligation to identify all customers, but must do so when they send or receive transactions of $3,000 or more for a customer. However, they must register with FinCEN[7] and renew this registration periodically thereafter. To the extent that virtual currency businesses become subject to the BSA, it is usually because they qualify as a money transmitter, and therefore, as an MSB.

Whether an entity or individual qualifies as a money transmitter is determined by the type of activities in which that person or entity engages. A money transmitter is a person "wherever located" that engages as a business "wholly or in substantial part in the United States" in the provision of money transmission[8] services. "Money transmission services" are defined to include "the acceptance of currency, funds, or other value that substitutes for currency from one person and the transmission of currency, funds, or other value that substitutes for currency to another location or person by any means."[9] "Any means" includes "through a financial agency or institution," such as the use of a bank account. This concept is very broad, both in the breadth of transactions potentially covered, and in the fact that it includes foreign entities that provide money transmission services to persons in the U.S.[10]

FinCEN Virtual Currency Guidance

Although the rules governing money transmitters were not established specifically with virtual currency in mind, they are drafted broadly and were intended to be adaptable to a wide variety of conduct. FinCEN has sought to fill in gaps in their interpretation within the specific context of virtual currencies by providing guidance on this issue, in particular two substantial pieces of guidance in March 2013 and May 2019.

In its 2013 Guidance, FinCEN explained that it defines "value that substitutes for currency" under the money transmission standard to include "convertible virtual currency."[11] The Guidance defines virtual currency as "a medium of exchange that operates like a currency in some environments, but does not have all the attributes of real currency."[12] A convertible virtual currency is one that "has an equivalent value in real currency, or acts as a substitute for real currency."[13] Perhaps most importantly, FinCEN treats the exchange of fiat currency for virtual currency as the transmission of "currency, or value that substitutes for currency" from one location – the purchaser's fiat wallet – to another, i.e., a new virtual currency wallet, and therefore as "money transmission."[14] The Guidance also identifies three categories of participants in the virtual currency ecosystem: users; exchangers; and administrators.[15]

- **User**: A person who "obtains virtual currency to purchase goods or services" is a user.[16] This includes businesses that are strictly investing in CVC for their own account and not for any other party.[17] Under the current guidance, institutions investing in virtual currencies, i.e., co-mingled investment funds, are likely considered users. The method of obtaining virtual currency (e.g., "earning," "harvesting," "mining," "creating," "auto-generating," "manufacturing," or "purchasing") is not determinative of whether a person qualifies as a "user," an "administrator," or an "exchanger."[18]
- **Exchanger**: "A person engaged as a business in the exchange of virtual currency for real currency, funds, or other virtual currency" is an exchanger.[19] Importantly, a person must be engaged as a business; thus, trading simply for personal investment purposes does not qualify one as an exchanger. In addition, one must accept and transmit virtual currency from one person to another or to another location. This covers transactions where the parties are exchanging fiat and CVC, and transactions where parties are exchanging one virtual currency for another virtual currency. However, the mere acceptance of virtual currency in exchange for providing a good or service does not make a person a money transmitter.
- **Administrator**: A person engaged as a business in issuing (putting into circulation) a virtual currency, and who has the authority to redeem (withdraw from circulation) such virtual currency, is an administrator.[20]

Users are not considered money transmitters, and are thus not required to register with FinCEN or otherwise comply with BSA regulations. Exchangers or administrators may be considered money transmitters and could be required to register with FinCEN and comply with BSA regulations, depending on the specific facts and circumstances of the entity's business model.

Classification of persons and entities conducting virtual currency business activities for money transmission purposes

Since issuing the March 2013 Guidance, FinCEN has issued subsequent guidance on virtual currency that further informs the application of existing money transmission regulations to various business models in the virtual currency arena, including the following:

Guidance

- *Application of FinCEN's Regulations to Certain Business Models Involving Convertible Virtual Currencies*, FIN-2019-G001 (May 9, 2019).
- *Advisory on Illicit Activity Involving Convertible Virtual Currency*, FIN-2019-A003 (May 9, 2019).

Administrative Ruling

- *Application of FinCEN's Regulations to Virtual Currency Software Development and Certain Investment Activity*, FIN-2014-R002 (Jan. 30, 2014) ("2014 Software and Investment Ruling").

- *Application of FinCEN's Regulations to Virtual Currency Mining Operations*, FIN-2014-R001 (Jan. 30, 2014) ("2014 Mining Ruling").
- *Request for Administrative Ruling on the Application of FinCEN's Regulations to a Virtual Currency Payment System*, FIN-2014-R012 (Oct. 27, 2014) ("2014 Payment System Ruling").

Below is a summary of how the FinCEN Guidance and the 2014 Payment System Ruling might apply to various players in the virtual currency market.

- **Anonymizing services**: Businesses providing anonymizing services (also known as "mixers" or "tumblers") that attempt to conceal the source of the transmission of virtual currency are money transmitters when they accept and transmit CVC and, therefore, have regulatory obligations under the BSA.[21]
- **Trading platforms and decentralized exchanges**: Peer-to-peer (P2P) trading platforms are websites where CVC buyers and sellers can connect. Sometimes, these platforms also facilitate trades as an intermediary. Under FinCEN regulations, a person is exempt from money transmitter status if the person only provides the delivery, communication, or network access services used by a money transmitter to support money transmission services.[22] Therefore, if a CVC trading platform only provides a forum where CVC buyers and sellers post their bids and offers (with or without automatic matching of counterparties), and the parties themselves settle any matched transactions through an outside venue (either through individual wallets or other wallets not hosted by the trading platform), the trading platform may not qualify as a money transmitter under FinCEN regulations. By contrast, if a trading platform accepts CVC from a seller and then sells it to the buyer, the trading platform is acting as a CVC exchanger, and thus falls within the definition of money transmitter and its accompanying BSA obligations.[23]
- **Software developer**: Whether software that facilitates the purchase or sale of virtual currency qualifies as money transmission for the developer depends on what the software does. Software that accomplishes the exchange of virtual currency between third parties is likely to be treated as money transmission by a developer or operator. Similar software that is used by a user to buy virtual currency for its own account may not be.[24]
- **Miners**: Miners play a vital role in allowing many decentralized blockchain-based virtual currency systems to operate properly. Mining is important because virtual currencies or tokens, i.e., Bitcoin, are initially acquired through mining. Unlike paper money, decentralized virtual currencies (DVCs) do not have a central government to issue the currency. This provides a somewhat controlled way to distribute tokens and creates a real incentive for miners to enter the market. Miners also play another vital role: in the traditional banking system, banks maintain an accurate record of parties and details of each transaction; however, since there is no central regulator for DVCs, the miners assume this role.

  Those who mine virtual currencies, whether by "earning," "harvesting," "creating," or "manufacturing," are classified as users – not money transmitters. Once the virtual currency is mined, a miner (depending on how he or she uses the CVC and for whose benefit) may potentially become a money transmitter.[25] Just because the miner acquired the tokens through mining, rather than purchasing or being given them, does not affect his or her status as a user. Moreover, miners may use their mined tokens or currencies to purchase goods for their own use or investment. However, miners that mine tokens for the purposes of operating a business as an exchanger of CVC for fiat currency, or for other forms of CVC, are likely to be subject to regulation as an exchanger.

- **Centralized virtual currencies**: A virtual currency that has a centralized repository is a centralized virtual currency. Such a repository is a money transmitter to the extent that it allows transfers of value between persons or from one location to another (e.g., a user's account in New York to that same user's account in California). In addition, if the centralized virtual currency repository accepts currency or its equivalent from a user, privately credits the user with an appropriate portion of the repository's own CVC and then transmits that internally credited value to third parties at the user's direction, the centralized virtual currency repository is a money transmitter.[26]
- **Decentralized virtual currencies**: A DVC has no central repository and no single person who has the ability to issue or redeem the virtual currency. Persons may obtain the virtual currency through their own computing or mining effort, or by purchasing the virtual currency. A person who creates units of a DVC and uses it to purchase real or virtual goods or services is a "user" of the DVC and is not subject to regulation as a money transmitter. By contrast, a person who creates units of a DVC, sells those units to another person for real currency or its equivalent and is engaged in that exchange as a business, is a money transmitter.
- **Natural persons providing CVC money transmission (P2P exchangers)**: FinCEN defines "money transmitter" to include both natural and legal persons engaged as a business in money transmission "whether or not on a regular basis or as an organized business concern."[27] P2P exchangers are generally natural persons engaged in the business of buying and selling CVCs. P2P exchangers facilitate transfers from one type of CVC to a different type of CVC, as well as exchanges between CVC and other types of value. P2P exchangers may provide their services online or in person. As the phrase quoted above suggests, a natural person operating as a P2P exchanger who engages in for-profit money transmission services involving real currency or CVCs is a money transmitter and must comply with BSA regulations, even if that person does not consider themselves to be a "real" business. FinCEN recently took enforcement against an individual running such an exchange without registering as a money transmitter.[28] There is a narrow exemption for a natural person that engages in money transmission "on an infrequent basis and not for gain or profit," but for-profit activities fall outside of this.[29] As a money transmitter, P2P exchangers are required to comply with BSA obligations that apply to money transmitters, including registering with FinCEN as an MSB and complying with the associated AML program, recordkeeping and reporting requirements. (This includes filing SARs and Currency Transaction Reports.)[30]
- **Wallets**: Wallets are virtual currency storage systems used to hold, send, or receive virtual currency. Most virtual currencies have official or suggested wallets and the use of one is necessary. The wallet contains a public and private key for each virtual currency address. The private key is a secret number that allows the virtual currency to be spent. The public key, which is mathematically derived from the private key, is used to ensure that the wallet holder is the owner of the wallet address and can receive funds. The status of a wallet provider as a money transmitter is affected by whether it has custody of the private keys for the virtual currency, which affects whether the wallet provider is deemed to have accepted and transmitted the funds sent using that key.
- **Custodial exchanges**: Custodial exchanges are virtual currency exchange platforms on which users are able to buy and sell virtual currencies. What distinguishes this type of exchange as custodial is the fact that the exchange is in control of a user's funds. In other words, the exchange is the custodian of the private keys for the virtual currencies or tokens. Custodial exchanges are typically money transmitters because they are buying, selling, accepting and transmitting virtual currencies.

- **Non-custodial "exchanges"**: Companies that act merely as platforms to connect buyers and sellers of CVC but which do not accept funds from customers or hold or control private keys for customer CVC are less likely to qualify as money transmitters. Such services may act more akin to a message or classifieds board like Craigslist. Because they are never in possession of the currency or private keys, they are less likely to be considered to accept, transmit, buy or sell virtual currencies.
- **Token issuers**: FinCEN has indicated that those who raise money through an initial coin offering by accepting fiat currency or other value in exchange for an immediate or subsequent distribution of CVC qualify as money transmitters.[31] By contrast, an issuer that merely gives away or "air drops" such tokens may not be subject to regulation because tokens were not exchanged for another form of value.
- **Payment systems**: Virtual currency payment processing systems typically process payments and assist in executing transactions by accepting fiat from the buyer, keeping that fiat, and then paying the seller with the approximate market value of a virtual currency, or *vice versa*. By keeping a large reserve of virtual currency at all times, the payment processer is able to act as his or her own currency exchange to supply equivalent virtual currency in exchange for the fiat supplied by the buyer.

  According to FinCEN, payment processing systems that accept and convert both real and virtual currencies are money transmitters because they are exchangers and, therefore, must register.[32] An exchanger will be subject to the same obligations under FinCEN regulations regardless of whether it acts as a broker – attempting to match two essentially simultaneous and offsetting transactions involving the acceptance of one type of currency and the transmission of another – or as a dealer – transacting from its own reserve in either convertible virtual currency or real currency.[33]

  There is, however, a carve-out from registration for payment processors when these four conditions are met:

  (i) The entity providing the service facilitates the purchase of goods or services, or the payment of bills for goods or services (other than money transmission itself).
  (ii) The entity operates through clearance and settlement systems that admit only BSA-regulated financial institutions.
  (iii) The entity provides the service pursuant to a formal agreement.
  (iv) The entity's agreement must be at a minimum with the seller or creditor that provided the goods or services and receives the funds.[34]
- **Bitcoin ATMs**: Generally, a fiat currency automated teller machine (ATM) is not subject to FinCEN regulations as an MSB or money transmitter.[35] Fiat ATMs simply allow a consumer to access his or her own account and his or her own fiat currency. There is no exchange because most fiat ATMs are unable to transmit funds to third parties or accounts at other financial institutions.[36] However, Bitcoin ATMs are not merely an intermediary between a consumer and his or her personal bank account. Bitcoin ATMs function as either one-way (converting fiat currency to Bitcoin) or two-way (converting fiat currency to Bitcoin and Bitcoin to fiat currency) machines. In both instances, these machines may act as intermediaries between buyers and sellers – more as brokers than as tellers. Therefore, Bitcoin ATM operators generally must register with FinCEN as money transmitters.
- **Internet casinos**: Internet casinos are virtual platforms that often accept bets and issue payouts denominated in CVC. Any internet casino that accepts and transmits value denominated in CVC may be regulated under the BSA as a money transmitter, and perhaps as a casino. Casinos are another form of "financial institution" subject to BSA rules, in addition to any laws and regulations applicable to gambling.[37]

Registering as a money services business

Persons engaged in money transmission have 180 days to register with FinCEN.[38] Any company or individual serving as an MSB must file a FinCEN Form 107, along with an estimate of business volume for the coming year, information related to the business' ownership and control, and a list of its authorized agents.[39] FinCEN Form 107 requires MSBs to identify: the states in which they have agents and branches; the type of money services activities they plan to carry out (e.g., money transmitter, currency dealer or exchanger, check casher); the number of agents they have authorized to carry out each activity; and the location (financial institution and account number) of their primary transaction account.[40] If accepted, registration must be renewed every two years. Should there be any change in ownership or control, transfer of a 10% voting or equity interest, or more than a 50% increase in authorized agents, then the business must re-register.[41]

Willful failures to comply with the reporting, recordkeeping and AML program requirements for money transmitters can result in penalties of up to $236,071.[42] The failure to maintain an appropriate AML program can result in a civil penalty of up to $57,317 per day the violation persists. The U.S. Department of Justice prosecutes criminally willful violations of the BSA, and such violations can result in criminal fines of up to $250,000 per violation, imprisonment for up to five years, or both.[43] It is also a felony to operate a money transmitter without required federal or state registrations or licenses.[44] While federal registration is relatively easy, once registered, ongoing BSA compliance obligations can be substantial.

No action letters/requests for rulings to federal or state regulators

If a person or entity is clearly a money transmitter, then federal registration with FinCEN is required, as is potential state licensing, which is discussed below. However, there may be situations in which it is unclear whether a person or entity must register as a money transmitter. In such circumstances, a person may request an administrative ruling from FinCEN.[45] A positive determination that a particular business model is not subject to regulation under the BSA can be an important asset. But FinCEN can take a considerable amount of time to grant such a determination, and may reach a different result from what the business wanted.

State virtual currency money transmission

State money transmission, unlike federal money transmission, requires licensure, not registration. As a prerequisite to receiving a license and/or in connection with maintaining a license, states generally require some combination of the following: payment of licensing costs; bonding; minimum-net-worth requirements; disclosure of applicants' employment history; submission to investigations or examinations; audited financials and periodic financial reporting; prior money transmission or financial services business experience; disclosure of litigation and bankruptcy proceedings; and fingerprinting and background checks.

Importantly, even if a person or entity is not a money transmitter under the BSA, they may be a money transmitter in any number of states, or *vice versa*.

A license is required in any state where the person or company does business or solicits citizens, regardless of whether he/she/it has any physical presence in the state. Thus, any entity that is planning a global or nationwide rollout of its virtual currency business must satisfy state licensing requirements regardless of where the entity is physically located. Because virtual currency is a borderless medium of exchange, this typically requires an analysis of, and possible licensure in, all 50 states in the U.S. and the District of Columbia.

Whether a particular entity is required to obtain a license in any state depends heavily on the specifics of the entity's business model. The analysis below is meant to provide an overview of whether licensure may be required in a given state for entities engaged in certain virtual currency activities. In many instances, we indicated that a particular state has taken no position on the applicability of its money transmission regulations to virtual currency businesses. However, in many of these states, a conservative reading of the definition of money (not necessarily limited to sovereign currency), monetary value (generally defined as "a medium of exchange, whether or not redeemable in money"), stored value (generally defined as "monetary value that is evidenced by an electronic record"), or a payment instrument (generally includes "an electronic instrument or order for the transmission or payment of money whether or not the instrument is negotiable") would require a virtual currency business to obtain a license. In light of this, some virtual currency businesses have obtained a traditional money transmitter license in certain states. Any analysis of applicable licensure requirements is inherently fact-specific, necessitating a detailed application of an entity's business model to the particular statutes and guidance in any given state. Due to these intricacies of state money transmission law and the uncertain applications of such laws to virtual currency activities, we recommend that you consult with counsel when determining whether state licensure is required.

State-level analysis

Alabama: Requires a license to transmit virtual currencies because virtual currencies are considered "monetary value," which is subject to regulation.[46]

Alaska: Requires virtual currency money transmitters to enter into a Limited License Agreement with the Alaska Department of Commerce, Community and Economic Development, Division of Banking and Securities.[47]

Arizona: The state has taken no position on virtual currency money transmission as of this chapter's date of publication.[48] In 2018, Arizona established a regulatory sandbox for the purpose of "enabl[ing] a person to obtain limited access to the market in this state to test innovative financial products or services without obtaining a license or other authorization that otherwise might be required."

Arkansas: The state has taken no position on virtual currency money transmission as of this chapter's date of publication.[49]

California: The California Department of Business Oversight (CDBO) released several opinion letters in 2019 and 2020 covering virtual currency.[50] Many of the opinions reflect that the CDBO has not yet determined whether virtual currencies are a form of money that triggers the application of the California Money Transmission Act and whether companies that deal in virtual currency need to be licensed and supervised. The opinion letters apply to various virtual currency businesses, including virtual currency escrow accounts and exchanges, virtual currency ATMs, virtual currency exchange platforms, companies seeking to receive virtual currency donations, and mobile-payments networks that allow consumers to use virtual currencies to pay for goods and services in California. The opinion letters are fact-specific and caution should be used in relying upon them. California Assembly Bill 1489, the Uniform Regulation of Virtual-Currency Businesses Act, was introduced by the legislature but has not been passed.[51]

Colorado: Requires a license to transmit virtual currency to the extent that the virtual currency transactions also involve the transfer of fiat currency.[52]

Connecticut: Requires a license to transmit virtual currency.[53]

Delaware: Requires a license to transmit virtual currency.[54]

District of Columbia: The District has taken no position on virtual currency money transmission as of this chapter's date of publication. However, caselaw suggests that money transmission laws reach cryptocurrencies since they qualify as "money."[55]

Florida: Requires a license to transmit virtual currency to the extent that the virtual currency transactions also involve the transfer of fiat currency.[56] Also, in January 2019, a Florida appellate court ruled that the state's money transmitter laws apply to a business engaging in the sale of Bitcoin because Bitcoin is a "payment instrument," *State v. Espinoza*, 264 So. 3d 1055 (Fla. Dist. Ct. App. 2019). In 2020, Florida created a financial technology sandbox within the Office of Financial Regulation to allow financial technology innovators to test new products and services in a supervised, flexible regulatory sandbox using exceptions to specified general law and waivers of the corresponding rule requirements under defined conditions.

Georgia: Requires a license to transmit virtual currency.[57]

Hawaii: Requires a license to transmit virtual currency.[58] SB2594 was introduced to the legislature in January 2020 with bipartisan backing, which would make it legal for Hawaiian banks to hold "digital securities," "virtual currencies," "digital consumer assets" and other "open blockchain tokens" for their customers. It would further authorize Hawaiian courts to hear digital asset claims. In August 2020, Hawaii announced that 12 virtual currency firms were selected to pilot Hawaii's digital currency regulatory sandbox, which allows virtual asset service providers to do business in the state without obtaining a money transmitter license for a two-year period. The pilot program is offered through the Digital Currency Innovation Lab, a partnership between Hawaii's Department of Financial Institutions and the Hawaii Technology Development Corporation.

Idaho: Entities that operate an exchange or trade platform that allows users to exchange one digital currency for another – but that do not allow trading in or deposits of fiat currency – do not require a license. An entity that sells its own inventory of virtual currency does not require a license, but an entity that holds customer funds while arranging an exchange with a third party and transmits virtual currency between the parties does require a license.[59]

Illinois: Requires a license to transmit virtual currency to the extent that the virtual currency transactions also involve the transfer of fiat currency.[60]

Indiana: Requires a license to transmit virtual currency to the extent that the virtual currency transactions also involve the transfer of fiat currency.[61]

Iowa: The state has taken no position on virtual currency money transmission as of the date of this chapter's publication.[62]

Kansas: Requires a license to transmit virtual currency to the extent that the virtual currency transactions also involve the transfer of fiat currency.[63]

Kentucky: The commonwealth has taken no position on virtual currency money transmission as of the date of this chapter's publication.[64]

Louisiana: On June 13, 2020, the Louisiana governor signed HB 701, which provides for the licensing and regulation of virtual currency businesses in the state. Subject to certain exceptions, the bill establishes licensing and registration requirements, and, among other things: (i) authorizes reciprocity of licensure with other states; (ii) specifies that licensee applications must be submitted through the Nationwide Multi-State Licensing System; (iii) adds provisions related to licensee examinations; (iv) outlines licensee surety bond requirements "based on the nature and extent of risks in the applicant's virtual currency business model;" (v) provides the state's office of financial institutions with enforcement authority; and (vi) prohibits licensees from engaging in unfair, deceptive, or fraudulent practices. The act became effective on August 1, 2020.[65]

Maine: The state has taken no position on virtual currency money transmission as of the date of this chapter's publication.[66]

Maryland: The state has suggested that it generally does not regulate virtual currency at this time.[67]

Massachusetts: The commonwealth generally does not regulate domestic money transmission. The state also exempts Bitcoin ATMs from "financial institution" and Bitcoins from foreign currency transmission regulations.[68] Businesses involved in the dissemination of virtual currencies on the internet are "marketplace facilitators" subject to sales or use tax collection.[69]

Michigan: The state has taken no position on virtual currency money transmission as of the date of this chapter's publication. Virtual currency transactions are exempt from sales tax, and retailers are required to instantly convert the value of the virtual currency to U.S. dollars as of the day and exact time of the transaction.[70]

Minnesota: The state has taken no position on virtual currency money transmission as of the date of this chapter's publication.[71]

Mississippi: The state has taken no position on virtual currency money transmission as of the date of this chapter's publication.[72]

Missouri: The state has taken no position on virtual currency money transmission as of the date of this chapter's publication, except that it exempts Bitcoin ATM transactions from sales tax.[73]

Montana: The state is the only U.S. jurisdiction that does not regulate money transmission.

Nebraska: The state has taken no position on virtual currency money transmission as of the date of this chapter's publication.

Nevada: Bitcoin ATM kiosks must be licensed by the state and will require a surety bond requirement. Certain other transactions in virtual currency may require licensure in Nevada. Nevada also created a sandbox program "to help businesses test innovative financial products or services without first having to meet certain state licensing or regulatory requirements."[74]

New Hampshire: The state exempts from licensure "persons who engage in the business of selling or issuing payment instruments or stored value solely in the form of convertible virtual currency or receive convertible virtual currency for transactions to another location."[75]

New Jersey: The state has taken no position on virtual currency money transmission as of the date of this chapter's publication.[76]

New Mexico: Requires a license to transmit virtual currency, to the extent that the virtual currency transactions also involve the transfer of fiat currency.[77]

New York: A license known as a BitLicense is required by the New York State Department of Financial Services (NYDFS) to engage in any "virtual currency business activity," which is broadly defined under the regulations but has certain significant exemptions.[78] On June 24, 2020, NYDFS launched a proposed conditional licensing framework, final guidance concerning a licensee's ability to self-certify the use of new coins and additional resources intended to help virtual currency market participants. NYDFS also requested comments on the proposed conditional licensing framework, which will allow an entity to apply for a conditional license when partnering with an existing NYDFS-authorized entity to engage in virtual currency business activity during the term of the conditional license.

North Carolina: Requires a license to transmit virtual currency.[79]

North Dakota: Requires a license to transmit virtual currency, to the extent that the virtual currency transactions also involve the transfer of fiat currency.[80]

Ohio: The state has not explicitly included "virtual currencies" or "monetary value" in its money transmitter statute and the state's Department of Commerce has not published guidance on virtual currency regulations. However, the Ohio Money Transmitter License New Application Checklist requires a third-party security audit if the applicant will engage in the transaction of virtual currency in the course of money transmission activities.[81]

Oklahoma: The state has taken no position on virtual currency money transmission as of the date of this chapter's publication. In 2019, HB 1954 (the URVCBA) was introduced by the legislature, but has not been passed.

Oregon: Requires a license to transmit virtual currency.[82]

Pennsylvania: The Pennsylvania Department of Banking and Securities has published guidance stating that virtual currency – including Bitcoin – is not considered "money" under the state's Money Transmitter Act (MTA). Only fiat currency or currency issued by the U.S. government is considered "money" under the MTA and to transmit money under the MTA, (i) fiat currency must be transferred with or on behalf of an individual to a third party, and (ii) the money transmitter must charge a fee for the transmission. Because virtual currency trading platforms (along with virtual currency kiosks, ATMs, and vending machines) never directly handle fiat currency and there is no transfer of money from a user to a third party, they are not money transmitters under the MTA and therefore do not need a license in order to operate in the state.[83]

Rhode Island: HB 5847 was signed into law effective January 1, 2020, which adds virtual currency to the existing electronic money transmission and sale of check license law, and adds additional provisions clarifying the licensing process. The bill renames Chapter 19-14.3 of Rhode Island's General Laws titled "Sale of Checks and Electronic Money Transfers" to "Currency Transmission" and includes virtual currency within the definition of currency transmission. The bill defines virtual currency as a "digital representation of value that: (A) [i]s used as a medium of exchange, unit of account, or store of value; and (B) [i]s not legal tender, whether or not denominated in legal tender." Among other things, the bill excludes from the definition of virtual currency a "[n]ative digital token used in a proprietary blockchain service platform." Subject to certain exceptions, the bill requires a person engaging in currency transmission business activity to be licensed with the state. Additionally, the bill: (i) requires virtual currency licensees to provide resident users of their services specified disclosures; (ii) subjects applicants and licensees to mandatory compliance programs and monitoring; and (iii) prohibits licensees from engaging in unfair, deceptive or fraudulent practices.[84]

South Carolina: To the extent that virtual currency transactions also involve the transfer of fiat currency, they may be subject to money transmission regulations under the Act.[85]

South Dakota: In May 2019, the state's Division of Banking issued guidance concluding that virtual currencies are "monetary value" as applicable by the state's Money Transmitter rules. Moreover, its Money Transmitter License New Application on NMLS authorizes virtual currency exchanging and trading services.

Tennessee: Tennessee guidance provides that transactions solely involving exchanges of cryptocurrency are not money under the Tennessee MTA. Even the exchange of cryptocurrency for sovereign currency or the exchange of one cryptocurrency for another between two parties is not money transmission. However, the exchange of cryptocurrency for sovereign currency through a third-party exchanger is generally considered money transmission. In addition, cryptocurrency ATMs may be considered money transmission under certain circumstances.[86]

Texas: The state has taken the position that certain virtual currency money transmission activities do not require licensure, while other transactions – including those involving virtual currency ATMs – may require licensure.[87]

Utah: "Blockchain tokens" are not within the scope of Utah's money transmission statute. In late 2019, Utah's governor signed into law HB 378, which created a sandbox program for companies providing "innovative financial products or services" in the state. Utah's sandbox allows participants to "temporarily test innovative financial products or services on a limited basis without otherwise being licensed or authorized to act under the laws of the state." The program is administered by the Utah Department of Commerce. Importantly, HB 378 specifically includes "blockchain technology" within its scope.[88]

Vermont: Requires a license to transmit virtual currency.[89]

Virginia: Requires a license to transmit virtual currency to the extent that the virtual currency transactions also involve the transfer of fiat currency.[90]

Washington: Requires a license to transmit virtual currency.[91]

West Virginia: The state has taken no position on virtual currency money transmission as of the date of this chapter's publication. During the 2020 Legislative Session, the West Virginia legislature passed and the governor signed HB 4621, which implements a regulatory sandbox to enable entities that would normally require licensure in West Virginia to test an innovative financial product or service for a limited period of 24 months.[92]

Wisconsin: Requires a license to transmit virtual currency, to the extent that the virtual currency transactions also involve the transfer of fiat currency under certain circumstances.[93]

Wyoming: The state exempts buying, selling, issuing, taking custody of payment instruments or stored value in the form of virtual currency, or receiving virtual currency for transmission from the Wyoming money transmitter licensure requirements.[94] In addition, the Wyoming legislature enacted HB 57 in 2019, which created a financial technology sandbox for the testing of innovative financial products and services in Wyoming. An "innovative financial product or service" is defined as a product or service that uses "new or emerging technology, or new uses of existing technology, that provides a product, service, business model or delivery mechanism to the public and has no substantially comparable, widely available analogue in Wyoming, including blockchain technology." Wyoming's sandbox is tailored to allow individuals and companies with new ideas to bring their product or service to market in a supportive environment that facilitates collaboration, consumer protection and innovation.[95]

Attempts to standardize licensing practices

The URVCBA establishes a regulatory structure for businesses engaging in, or offering to residents of enacting states, certain virtual currency transfer, exchange or custodial services. The URVCBA provides certainty and protections that will enable such businesses to operate to everyone's benefit. It includes provisions to enable start-up companies offering virtual currency services room to test products and operate prior to full licensure without violating state "money transmitter" or "money services" laws, or risking federal prosecution for being unlicensed under 18 U.S.C. § 1960.[96] The URVCBA has not been adopted although, as noted above, a few states are considering its adoption.

In July of 2018, the Office of the Comptroller of the Currency (OCC) announced that non-depository fintech firms engaged in a core banking function may apply for a special purpose national bank charter (Fintech Charter). Businesses with this charter may conduct

some financial service activities without state licenses, but will be subject to supervision and examination by the OCC. The Fintech Charter was promptly met with litigation from state and local government regulators in both New York and Washington, D.C., each of which raised similar legal challenges.[97] The Washington, D.C. case was dismissed, while on appeal, the Second Circuit in New York reversed and remanded to the District Court with instructions to dismiss with prejudice. To date, no company has applied for a charter, perhaps due to the uncertainty created by these pending legal challenges.

Acting Comptroller of the Currency Brian Brooks told various media outlets in July 2020 that the OCC plans to introduce a special purpose national bank charter (Payment Charter) that would give payment companies a nationwide servicing platform and federal preemption of state laws regarding licensing and regulation of money transmitters and payment services providers. The Payment Charter would be rolled out in two phases: first, a basic national money transmitter license; and second, direct access to the Federal Reserve's payments system, giving payment companies the ability to clear payments through the Federal Reserve System. As of the date of this chapter's publication, no additional information regarding the proposed Payment Charter was available.

In an attempt to simplify the process and to create some uniformity and efficiency, seven states – Georgia, Illinois, Kansas, Massachusetts, Tennessee, Texas, and Washington – have come together to reach a level of reciprocity.[98] In early 2018, these states agreed that if one party state reviews key requirements of state licensing for a money transmitter applicant, including cybersecurity, background checks and compliance with the BSA, then the other participating states will accept those findings in their own licensing process. This is the first real step toward an integrated 50-state system of licensure and supervision.

Most recently, on September 15, 2020, the Conference of State Bank Supervisors (CSBS) announced the launch of a "state-initiated program whereby nationwide payments firms will undergo a single comprehensive exam to satisfy all state regulatory requirements." The new regulatory regime will streamline licensing and ongoing compliance for MSBs operating in 40 or more states by requiring MSBs to undergo a single exam by a joint group of state regulators. The CSBS' new regulatory regime is intended to make it easier for MSBs to operate across multiple states.[99]

* * *

Endnotes

1. 12 U.S.C. § 1829b, 12 U.S.C. §§ 1951–1959, 18 U.S.C. § 1956, 18 U.S.C. § 1957, 18 U.S.C. § 1960, and 31 U.S.C. §§ 5311–5314 and 5316–5332.
2. FinCEN does not have criminal enforcement authority.
3. 31 U.S.C. §§ 5311–5332.
4. *See*, *e.g.*, 31 C.F.R. §§ 1020.320 (SAR requirement for banks); 1022.320 (SAR requirement for MSBs).
5. *See*, *e.g.*, 31 C.F.R. § 1020.320(a)(2)(iii); *cf*. Federal Financial Institutions Examination Council, Bank Secrecy Act/Anti-Money Laundering Examination Manual (2014), at Appendix F.
6. *See*, *e.g.*, 31 C.F.R. §§ 1020.210 (CDD requirement); 1020.220 (CIP requirement).
7. *See* 31 C.F.R. § 1022.380.
8. 31 C.F.R. § 1010.100(ff)(5).

9. 31 C.F.R. § 1010.100(ff)(5)(i)(A).
10. *See* 76. Fed. Reg. 43585, 43586, 43588 (July 21, 2011).
11. FinCEN, FIN-2013-G001 (Mar. 18, 2013) ("2013 Guidance"), at 1.
12. *Id*.
13. 2013 Guidance at 1.
14. 2013 Guidance at 4.
15. *Id*.
16. *Id.* at p. 2.
17. *Application of FinCEN's Regulations to Virtual Currency Software Development and Certain Investment Activity*, FIN-2014-R002 (Jan. 30, 2014).
18. *See also Application of FinCEN's Regulations to Virtual Currency Mining Operations*, FIN-2014-R001 (Jan. 30, 2014) (clarifying that a user is a person who obtains virtual currency to purchase goods or services on the user's own behalf).
19. *Id.* at p. 2.
20. FIN-2013-G001 p. 2.
21. *See also* https://www.fincen.gov/news/speeches/prepared-remarks-fincen-director-kenneth-blanco-delivered-2018-chicago-kent-block.
22. 31 C.F.R. § 1010.100(ff)(5)(ii)(A).
23. *See Request for Administrative Ruling on the Application of FinCEN's Regulations to a Virtual Currency Trading Platform*, FIN-2014-R011 (Oct. 27, 2014).
24. 2014 Software and Investment Guidance p. 2.
25. 2014 Mining Guidance.
26. FIN-2013-G001 p. 4.
27. 31 C.F.R. § 1010.100(ff).
28. FinCEN pursued enforcement action against Eric Powers in April 2019 for operating a peer-to-peer exchange for virtual currency without registering with FinCEN as a money transmitter. Mr. Powers advertised his intent to buy and sell Bitcoin on the internet, and completed transactions by physical delivery, mail or coordinating wires. Numerous of these transactions were also suspicious. FinCEN also levied a $35,000 fine against Mr. Powers and Mr. Powers agreed to an industry bar from providing money transmission services or other activity that would make him a money services business for purposes of FinCEN regulation.
29. 31 C.F.R. § 1010.100(ff)(8)(iii).
30. *See* FIN-2014-R002 (concerning the regulatory treatment of those persons investing in CVCs).
31. 2019 Guidance at 26; *see also* Letter from Drew Maloney, Assistant Secretary for Legislative Affairs, U.S. Department of the Treasury, to Senator Ron Wyden (Feb. 13, 2018) (explaining with respect to ICOs "that a developer that sells convertible virtual currency, including in the form of ICO coins or tokens, in exchange for another type of value that substitutes for currency, is a money transmitter").
32. 2014 Payment System Ruling.
33. *Id*.
34. 2014 Payment System Ruling p. 3.
35. *Application of the Definition of Money Services Business to Certain Owner-Operators of Automated Teller Machines Offering Limited Services*, FIN-2007-G006 (Dec. 3, 2007).
36. *Id*.
37. Definition of "financial institutions" to include casinos at 1010.100(t).

38. 31 C.F.R. § 1022.380.
39. 31 C.F.R. § 1022.380.
40. *See* FinCEN Form 107 (Mar. 2011).
41. 31 C.F.R. § 1022.380(b)(4).
42. 31 U.S.C. 5321; 86 Fed. Reg. 7348, 7349 (Jan. 28, 2021).
43. 18 U.S.C. § 1960.
44. *See* 18 U.S.C. § 1960(b)(1)(A), (B).
45. *See* 31 C.F.R. § 1010.711.
46. Ala. Code § 8-7A-1 *et seq.* (2017).
47. *See* https://www.commerce.alaska.gov/web/dbs/LimitedLicenseAgreementOrders.aspx (last visited Sept. 14, 2020).
48. Ariz. Rev. Stat. Ann. § 6-1201 *et seq.* (2014); A.R.S. §§ 41-5601–41-5612 (2018).
49. Ark. Code Ann. § 23-55-101 *et seq*. (West 2008).
50. *See* https://dbo.ca.gov/dfi-opinion-letters/.
51. In February 2019, Assembly Bill 1489 was introduced to the California legislature to enact the "Uniform Regulation of Virtual-Currency Businesses Act," which provides a statutory framework for the regulation of companies engaging in "virtual currency business activity," such as exchanging, transferring, or storing virtual currency, or exchanging digital representations of value within online games for virtual currency or legal tender. The bill has not been passed.
52. Colo. Rev. Stat. § 11-110-106 *et seq*. (West 2017); *see also* Interim Regulatory Guidance Cryptocurrency and the Colorado Money Transmitters Act, Colorado Department of Regulatory Agencies, Sept. 20, 2018, https://drive.google.com/file/d/1MmpksD8aAPkmvdRdW0PztGe_eOceq4lk/view. On March 6, 2019, Colorado enacted the "Colorado Digital Token Act." "The bill provides limited exemptions from the securities registration and securities broker-dealer and salesperson licensing requirements for persons dealing in digital tokens. "Digital token" is defined as a digital unit with specified characteristics, secured through a decentralized ledger or database, exchangeable for goods or services, and capable of being traded or transferred between persons without an intermediary or custodian of value." https://leg.colorado.gov/bills/sb19-023.
53. Conn. Gen. Stat. Ann. § 36a-595 *et seq*. (2013). A recently proposed House Bill would establish a regulatory sandbox allowing unlicensed or unauthorized testing of innovative products, including blockchain. 2021 CT HB 5761 (NS); HB 5210, 2020 Leg., 2020 Feb. Reg. Sess. Gen. Ass. (Conn. 2020).
54. *See generally* De. Code Ann. tit. 5, § 2303 (West 2020); https://nationwidelicensingsystem.org/slr/PublishedStateDocuments/CT_Money_Transmission_License-New-App-Checklist.pdf.
55. *See generally* D.C. mun. Regs. tit. 26 ch. 26C22 *et seq*. (2020); *United States v. Harmon*, 474 F. Supp. 3d 76 (D.D.C. 2020).
56. Fla. Stat. § 896.101 *et seq*. (West 2017); *see also* Florida Declaratory Statement No. 2018-538, 91969 (Nov. 19, 2018); Fla. Stat. § 559.952 (creating regulatory sandbox).
57. Ga. Code Ann. § 7-1-680 *et seq*. (West 2020).
58. Haw. Rev. Stat. Ann. § 489D-1 *et seq*. (West 2006); *see also* Hawaii Division of Financial Institutions News Release: State Warns Consumers on Potential Bitcoin Issues, Feb. 26, 2014, *available at* https://cca.hawaii.gov/dfi/news-releases/news-release-state-warns-consumers-on-potential-bitcoin-issues/ (last visited Sept. 15, 2020). Coinbase exited

Hawaii in 2017, requiring Hawaiian customers to close their accounts, stating that it would be impossible for Coinbase to operate in the state given the reserve requirement for money transmitters in the statute.

59. Idaho Department of Finance, Letter Dated March 12, 2018, *available at* https:// www.finance.idaho.gov/legal/no-action-opinion-letters/money-transmitter/documents/digital-currency/2018-03-09.pdf.
60. 205 Ill. Comp. Stat. Ann. § 657/1 *et seq*. (West 1995); *see also* Illinois Department of Financial and Professional Regulation, Digital Currency Regulatory Guidance (June 13, 2017), *available at* https://www.idfpr.com/Forms/DFI/CCD/IDFPR%20-%20Digital%20Currency%20Regulatory%20Guidance.pdf.
61. Ind. Code § 28-8-4-1 *et seq.* (2013); *see also* Money Transmitter License New Application Checklist, Ind. Dep't of Fin. Inst., *available at* http://nationwidelicensingsystem.org/slr/PublishedStateDocuments/IN-DFI-Money-Transmitter-Company-New-App-Checklist.pdf (last updated Mar. 10, 2020).
62. *See generally*, Iowa Code § 533C.102 *et seq.* (2003).
63. Kan. Stat. Ann. § 9-508 *et seq*. (West 2017). *See Regulatory Treatment of Virtual Currencies Under the Kansas Money Transmitter Act*, Kan. Off. of the State Bank Comm'r (June 6, 2014), *available at* http://www.osbckansas.org/mt/guidance/mt2014_01_virtual_currency.pdf.
64. *See generally* Ky. Rev. Stat. Ann. § 286.11-001 *et seq*. (West 2006).
65. HB 701, 2020 Reg. Sess. (La. 2020), codified at La. R.S. §§ 6:1381–6:1394 (eff. Aug. 1, 2020).
66. *See generally* Me. Rev. Stat. tit. 32, § 6101 *et seq*. (1997).
67. Md. Code Ann., Fin. Inst. § 12-401 *et seq.* (West 2014); *see Virtual Currencies: Risk for Buying, Selling, Transacting, and Investing – Advisory Notice 14-01*, Off. of the Comm'r of Fin. Regulation (Apr. 24, 2014), *available at* https://www.dllr.state.md.us/finance/advisories/advisoryvirtual.pdf.
68. Mass. Division of Banks, Opinion 14-004 (May 12, 2014). 63. 830 CMRH 1.7(b)(1), *available at* https://www.mass.gov/doc/selected-opinion-14-004/download (last visited Sept. 15, 2020).
69. Mass. Gen. Laws ch. 169, § 1 *et seq.* (West 1991); *see* Mass. Div. of Banks, Opinion 18-003 (June 14, 2018), *available at* http://www.mass.gov/files/documents/2018/06/21/Select%20Opinion%2018-003.pdf (last visited Sept. 15, 2020).
70. *See* Tax Policy Division of the Michigan Dept. of Treasury, Treasury Update, Vol. 1, Issue 1 (Nov. 2015), *available at* https://www.michigan.gov/documents/treasury/Tax-Policy-November2015-Newsletter_504036_7.pdf (last visited Sept. 14, 2020).
71. *See generally* Minn. Stat. § 53B.01 *et seq.* (2001).
72. *See generally* Miss. Code Ann. § 75-15-1 *et seq.* (West 2010).
73. Missouri Dep't of Revenue, LR 7411, Collection of Sales Tax on Bitcoin Transfers Through an Automated Teller Machine (ATM) (Sept. 12, 2014), *available at* http://dor.mo.gov/rulings/show/7411 (last visited Sept. 15, 2020).
74. https://business.nv.gov/News_Media/Press_Releases/2019/Financial_Institutions/Nevada_Financial_Institutions_Division_statement_on_regulation_of_cryptocurrency_in_Nevada/; https://business.nv.gov/Programs/Nevada_Sandbox_Program/.
75. N.H. Rev. Stat. Ann. § 399-G:3 (2017).
76. *See generally* N.J. Stat. Ann. § 17:15C *et seq.* (1998).
77. N.M. Stat. Ann. § 58-32-101 *et seq*. (West 2017); *see also* Money Transmitter License New Application Checklist, New Mexico Financial Institutions Division, *available*

at https://nationwidelicensingsystem.org/slr/PublishedStateDocuments/NM_Money_Transmission_License-Company-New-App-Checklist.pdf.

78. 23 N.Y. Comp. Codes R. & Regs § 200. The New York State regulatory scheme has been the subject of much criticism and has resulted in an exodus of businesses from New York because of the costs and regulatory requirements associated with the BitLicense. As of the date of this chapter, 18 companies have been granted a BitLicense. *See also* https://www.dfs.ny.gov/reports_and_publications/press_releases/pr202006241 (last visited Sept. 15, 2020).
79. N.C. Gen. Stat. § 53-208.41 *et seq.* (2016).
80. N.D. Cent. Code § 13-09-01 *et seq.* (West 2005). *See Frequently Asked Questions – Non-Depository: Money Transmitters*, N.D. Dep't of Fin. Insts. (2018), https://www.nd.gov/dfi/about-dfi/non-depository/frequently-asked-questions-non-depository.
81. https://nationwidelicensingsystem.org/slr/PublishedStateDocuments/OH-Money-Transmitter-Company-New-App-Checklist.pdf.
82. Or. Rev. Stat. Ann. § 717.205 *et seq*. (West 2018).
83. *Money Transmitter Act Guidance for Virtual Currency Businesses*, Pa. Dep't of Banking and Secs. (Jan. 2019).
84. *See* R.I. HB 5847 (2019).
85. *See* South Carolina Attorney General, *Money Services Frequently Asked Questions*, *available at* http://www.scag.gov/money-services-frequently-asked-questions (last visited July 14, 2021); *see also* http://2hsvz0l74ah31vgcm16peuy12tz.wpengine.netdna-cdn.com/wp-content/uploads/2019/02/01845729.pdf.
86. *See* Memo, Tenn. Dep't of Fin. Inst., *Regulatory Treatment of Virtual Currencies under the Tennessee Money Transmitter Act* (Dec. 16, 2015), *available at* https://www.tn.gov/content/dam/tn/financialinstitutions/new-docs/TDFI%20Memo%20on%20Virtual%20Currency.pdf (last visited Sept. 14, 2020).
87. *See* Texas Dep't of Banking, Supervisory Memorandum 1037, *Regulatory Treatment of Virtual Currencies Under the Texas Money Services Act*, *available at* https://www.dob.texas.gov/sites/default/files/files/consumer-information/sm1037.pdf (last visited Sept. 14, 2020).
88. *See* https://commerce.utah.gov/sandbox.html.
89. Vt. Stat. Ann. tit. 8, § 2500 *et seq*. (West 2019).
90. Va. Code Ann § 6.2-1900 *et seq*. (West 2019); *see also* Va. State Corp. Comm., *Notice to Virginia Residents Regarding Virtual Currency*, *available at* https://www.scc.virginia.gov/getattachment/1bb52b42-9a10-45a2-ba48-b352e48b6d2e/virtcur.pdf (last visited Sept. 14, 2020).
91. Wash. Rev. Code § 19.230.010 *et seq*. (West 2017).
92. W. Va. Code § 61-15-1 *et seq*. (West 2017); https://dfi.wv.gov/fintech/Pages/default.aspx.
93. Wis. Stat. § 217.01 *et seq*. (West 2019); *see also* https://www.wdfi.org/fi/lfs/soc/ (last visited Sept. 14, 2020).
94. Wyo. Stat. Ann., § 40-22-101 *et seq*. (West 2003); *see also* http://wyomingbankingdivision.wyo.gov/home/areas-of-regulation/laws-and-regulation/financial-technology-sandbox.
95. http://wyomingbankingdivision.wyo.gov/home/areas-of-regulation/laws-and-regulation/financial-technology-sandbox.
96. *See* https://www.uniformlaws.org/HigherLogic/System/DownloadDocumentFile.ashx?DocumentFileKey=de52d1fe-1f70-a568-9552-d354ade157ca&forceDialog=0.

97. *See Lacewell v. Office of the Comptroller of the Currency*, Case 1:18-cv-08377-VM (S.D.N.Y.) (ECF No. 45); *Conference of State Bank Supervisors v. Office of the Comptroller of the Currency*, No. 18-cv-2449 (DLF) (D.D.C.).
98. *See* Conf. of State Bank Supervisors, *State Regulators Take First Step to Standardize Licensing Practices for Fintech Payments* (Feb. 6, 2018), *available at* https://www.csbs.org/state-regulators-take-first-step-standardize-licensing-practices-fintech-payments (last visited Sept. 14, 2020).
99. *State Regulators Roll Out One Company, One Exam for Nationwide Payments Firms* (Sept. 15, 2020), *available at* https://www.csbs.org/regulators-announce-one-company-one-exam-for-payments-companies.

* * *

Acknowledgment

The authors acknowledge with thanks the contributions to this chapter by Joshua Durham.

Michelle Ann Gitlitz
Tel: +1 212 895 4334 / Email: mgitlitz@crowell.com

Michelle Gitlitz is the Global Head of Crowell & Moring's Blockchain and Digital Assets practice, and a partner in the White Collar & Regulatory Enforcement and Corporate groups. An experienced regulatory lawyer and litigator, Michelle's practice focuses on the legal and regulatory issues facing both emerging and established companies that invest in and incorporate blockchain technology and digital assets into their businesses. Her experience includes: advising clients on the legal, regulatory, and risk management issues surrounding coin/token offerings (including launching new offerings and remediating prior offerings); working with clients in connection with digital currency exchanges and platforms; establishing new blockchains and nodes; and advising clients on navigating federal and state money transmission laws.

Carlton Greene
Tel: +1 202 624 2818 / Email: cgreene@crowell.com

Carlton Greene is a partner in Crowell & Moring's Washington, D.C. office and a member of the firm's White Collar & Regulatory Enforcement and International Trade groups. He provides strategic advice to clients on U.S. economic sanctions, Bank Secrecy Act and anti-money laundering (AML) laws and regulations, export controls, and anti-corruption/anti-bribery laws and regulations. Carlton is the former chief counsel at FinCEN (the Financial Crimes Enforcement Network), the U.S. AML regulator responsible for administering the Bank Secrecy Act. Before joining FinCEN, Carlton previously served as the assistant director for transnational threats with the U.S. Department of the Treasury, Office of Foreign Assets Control (OFAC), where he directed targeting and investigations for more than 15 U.S. economic sanction programs, including those related to Iran and North Korea. Carlton also served as legal counsel to OFAC on counterterrorism sanctions.

Caroline Brown
Tel: +1 202 624 2509 / Email: cbrown@crowell.com

Caroline E. Brown is a partner in Crowell & Moring's Washington, D.C. office and a member of the firm's White Collar & Regulatory Enforcement and International Trade groups. She provides strategic advice to clients on national security matters, including anti-money laundering (AML) and economic sanctions compliance and enforcement challenges, cybersecurity, cross-border data transfers, and investigations. Caroline also advises companies navigating review by the Committee on Foreign Investment in the United States (CFIUS). Caroline brings over a decade of experience as a national security attorney at the U.S. Departments of Justice and the Treasury. Most recently, she served as an Attorney-Advisor in the Treasury Department's Financial Crimes Enforcement Network (FinCEN), where she developed an in-depth understanding of AML regulation and enforcement and FinCEN's role in guarding the U.S. financial system against money laundering and terrorism financing.

Crowell & Moring LLP

590 Madison Avenue, 20th Floor, New York, NY 10022-2544, USA
Tel: +1 212 223 4000 / Fax: +1 212 223 4134 / URL: www.crowell.com

Decentralized finance: Ready for its "close-up"?

Lewis Cohen, Angela Angelovska-Wilson & Greg Strong
DLx Law

Unstoppable code

Smart contract code deployed to a functioning blockchain network is unstoppable. Decentralized finance ("**DeFi**") protocols are suites of smart contracts – executable code accessible to anyone with the technical and practical capability to interact with that code – that allow users to transact value with others over the Internet with deterministic certainty yet without the need for one or more intermediaries. So long as the blockchain networks on which these smart contracts are deployed remain operational, the related DeFi protocols will be accessible.

There was more than the equivalent of US$92 billion of total value in digital assets "locked" in (*i.e.*, committed to) DeFi protocols as of September 16, 2021.[1] That amount of value, combined with the ability of users to conduct financial transactions pseudonymously without identification by an intermediary, is prompting regulators around the world to scrutinize the DeFi space. A global effort is under way to bring DeFi within (or at least closer to) the regulatory frameworks that apply to traditional finance. Whether and how this can be achieved in the context of unstoppable code remains very much an open question.

While the execution of blockchain-based smart contract code may be unstoppable, the individuals and businesses who develop the code and provide user-friendly access to that code are not. Our traditional regulatory frameworks focus on people – typically issuers and intermediaries – and there is a movement to bring those that develop, provide access to, or benefit economically from the operation of, the smart contracts comprising DeFi protocols within those existing regulatory definitions.

The development of DeFi forces regulators and market participants alike to confront some challenging questions: When should an individual or entity involved in developing smart contracts for DeFi protocols be held responsible for the outcomes of that code, especially when vulnerabilities in the code (leading to exploits and financial loss) are exposed? Should developers of the smart contracts or those who financed the development and who benefit economically through the ownership of related digital assets be required to take responsibility for the regulatory compliance of the protocols? What about a person or entity that simply provides access to such protocols through a website or application? Should regulators attempt to shoehorn developers and others into existing regulatory definitions that may not really fit in order to bring them within the ambit of existing regulatory frameworks, particularly when DeFi protocols are designed to eliminate traditional intermediaries? Alternatively, should brand-new regulatory frameworks be developed to meet the challenge of DeFi? These tricky questions are illustrative of the challenges in regulating actors contributing to DeFi as issuers or intermediaries.

Many now agree that DeFi needs regulation to evolve and grow. Not all current or future users of DeFi protocols will be sophisticated enough to fully evaluate the underlying smart contract code for themselves and will rely on others for this work. It is not hard to see that these users should benefit from protections. In addition, open peer-to-peer ("**P2P**") protocols allowing pseudonymous access can readily be used by bad actors for nefarious purposes, something that concerns all of us. That said, policymakers will need to be creative in approaching these developments. Yesterday's regulatory solutions will not be sufficient to address today's technologies. Efforts to encourage the development of regulation that is tailored to the unique nature of this technology to foster responsible growth and development must be encouraged. New approaches to regulation will provide more effective protection for the users of DeFi as well as clarity to actors contributing to these protocols with respect to their regulatory responsibilities.

Regulation of issuers and intermediaries

Regulation in the traditional finance world focuses on issuers and intermediaries. Our securities laws regulate issuers of securities and securities intermediaries that facilitate securities transactions. Our commodities laws regulate intermediaries that facilitate transactions in commodity derivatives and entities that offer commodity derivative contracts. Our financial regulatory laws, such as the Bank Secrecy Act (the "**BSA**"), apply to financial institutions broadly and require transaction monitoring, reporting, and recordkeeping in a variety of contexts. All of these frameworks are implicated by developments in DeFi.

Securities laws

Our securities laws regulate issuers of securities and intermediaries involved in securities transactions. Issuers of securities are generally required to disclose important information about the securities they intend to sell and their financial condition such that prospective investors can make informed investment decisions.[2] This information must be accurate and complete.[3] The level of detail required depends on whether the offering is registered and sold publicly[4] or whether it is exempt from registration and sold to limited numbers of persons or limited in size.[5] In addition to the disclosure requirements in connection with the initial sale of securities, issuers of public securities with 300 or more shareholders, and issuers with more than US$10 million in assets with securities held by more than 500 owners, must file annual and other periodic reports as well.[6]

Our securities laws also regulate intermediaries such as broker-dealers, transfer agents, clearing agencies, national securities exchanges, and investment advisors. Generally, each of these intermediaries must register with the Securities and Exchange Commission (the "**SEC**") and comply with the laws and regulations applicable to their activities as intermediaries.[7] The obligation of an entity to register with the SEC as one of the above-listed intermediaries is triggered by engaging in the regulated activity with respect to securities. For example, whether the assets that are being brokered are securities will determine whether registration as a broker-dealer is required.

Commodities laws

The Commodities Exchange Act (the "**CEA**") and related regulations regulate the trading of commodity derivatives.[8] One important component of this regulatory scheme is the registration and oversight of intermediaries who act on behalf of others in connection with commodity derivatives. There are a variety of intermediaries regulated under the CEA, including Commodity Pool Operators, Commodity Trading Advisors, Futures Commission Merchants, Introducing Brokers, Major Swap Participants, and Swap Dealers.[9] In addition, the CEA generally requires that many commodity derivatives be traded on a designated

contract market ("**DCM**").[10] DCMs are also licensed and regulated by the Commodity Futures Trading Commission (the "**CFTC**") and allow the CFTC to oversee transactions in commodity derivatives available to retail market participants.[11]

The BSA

The BSA mandates that "financial institutions,"[12] intermediaries who act on behalf of others in connection with financial transactions, collect and retain information about their customers and their transactions, and share that information with the Financial Crimes Enforcement Network ("**FinCEN**"). The BSA and its implementing regulations require the registration of a money services business ("**MSB**") within 180 days of beginning operations and the renewal of such registration every two years,[13] and require an MSB to develop, implement, and maintain an effective written anti-money laundering ("**AML**") program that is reasonably designed to prevent the MSB from being used to facilitate money laundering and the financing of terrorist activities.[14] An MSB is required to implement a written AML program that, at a minimum: (a) incorporates policies, procedures and internal controls reasonably designed to assure ongoing compliance; (b) designates an individual responsible to assure day-to-day compliance with the program and BSA requirements; (c) provides training for appropriate personnel, including training in the detection of suspicious transactions; and (d) provides for independent review to monitor and maintain an adequate program.[15]

In particular, when money transmitters process transactions that involve a "transmittal of funds,"[16] the Funds Travel Rule[17] applies to those transactions. Under the regulatory framework established under the BSA, a transmittal of funds is initiated by a "transmittal order," which is an instruction to pay funds to a recipient. The Funds Travel Rule requires that each of the financial institutions in a chain of transmittal orders involved in a transmittal of funds of US$3,000 or more originated by customers and non-customers maintain accurate records relating to the funds transfer and verify the identity of non-customers originating funds transfers.[18] The information required to be maintained depends on the role of the financial institution in the payment chain, *i.e.*, originator, intermediary, or beneficiary institution.[19] Financial institutions acting as originator or intermediary financial institutions must cause the information to "travel" to the next financial institution.[20]

FinCEN 2019 Guidance

On May 9, 2019, FinCEN, a division of the U.S. Treasury Department, issued guidance entitled "Application of FinCEN's Regulations to Certain Business Models Involving Convertible Virtual Currencies" (the "**Guidance**").[21] FinCEN is the arm of the Treasury Department responsible in the first instance for enforcing the U.S. federal laws and regulations relating to the transmission of money, including the BSA, frequently working in conjunction with other federal agencies and bureaus, including the Federal Bureau of Investigation and the National Security Agency. The Guidance was designed to consolidate current regulations, administrative rulings, and earlier guidance related to MSBs, with a focus on money transmission involving convertible virtual currency ("**CVC**").

While the Guidance touches on a number of different areas, two key areas include: (1) how the Funds Travel Rule applies to certain transactions involving CVCs and whether any such transactions trigger regulatory obligations under U.S. federal law for any participants who may be considered "money transmitters;" and (2) the application of relevant U.S. laws and regulations with respect to "decentralized" systems.[22] With respect to the former, the Guidance indicates that the Funds Travel Rule applies to transactions in CVCs.[23] Accordingly, any intermediary financial institution involved in the transmission of funds must provide certain information to the receiving financial institution, but they have no duty

to obtain information not provided by the transmitter's financial institution or the preceding financial institution.[24] The recipient's financial institution must receive, evaluate, and store the information received from the transmitter's financial institution or the intermediary financial institution.[25]

The key question is whether there are intermediaries in a given transaction that meet the definition of financial institution and are subject to the Funds Travel Rule. In the context of centralized intermediaries, the analysis is straightforward. In the context of automated transactions in decentralized systems, it is more difficult to identify an intermediary to hold responsible for compliance. The Guidance addresses the responsibility of developers/contributors to decentralized systems.[26] Under Section 5.2.2 of the Guidance, decentralized application ("**DApp**") developers are not regulated as money transmitters for "the mere act of creating the application, even if the purpose of the DApp is to issue a CVC or otherwise facilitate financial activities denominated in CVC," but they may be regulated as money transmitters if they "use" or "deploy" it "to engage in money transmission."[27] The Guidance is explicit about the application to decentralized systems and makes multiple references to unincorporated organizations coming within the ambit of the BSA in reference to decentralized systems. The Guidance goes on to specifically address DApps in the discussion of business models involving CVC money transmission, reiterating that the same rules apply there as well.[28]

DeFi contributors as issuers or intermediaries

Increasingly, regulators have sought to shoehorn DeFi participants into the existing regulatory frameworks described above by branding them intermediaries. This is true with respect to U.S. securities, commodities, and financial regulatory laws.

FATF virtual asset guidance

The issue of information reporting in connection with virtual asset transfers is at center stage internationally. In the Fall of 2018, the Financial Action Task Force ("**FATF**"), a multi-governmental organization that sets global standards related to AML, proposed amended Recommendation 15, which addresses new technologies to clarify how the FATF standards apply to activities or operations involving virtual assets.[29] Subsequently, FATF released an Interpretive Note to Recommendation 15.[30] Paragraph 7(b) of the Interpretive Note seeks to impose a corollary to the Funds Travel Rule on Virtual Asset Service Providers ("**VASPs**") processing virtual asset transfers.[31] The Interpretive Note was finalized in June 2019 following private sector consultations.[32]

More recently, FATF released new proposed updated guidance regarding virtual assets and VASPs, which is currently open for comment (the "**Updated FATF Guidance**").[33] A VASP "is 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 virtual assets and fiat currencies;
ii. Exchange between one or more forms of virtual assets;
iii. Transfer of virtual assets;
iv. Safekeeping and/or administration of virtual assets or instruments enabling control over virtual assets; and
v. Participation in and provision of financial services related to an issuer's offer and/or sale of a virtual asset."[34]

Notably, the Updated FATF Guidance seeks to make clear that the definitions of "Virtual Asset" and "VASP" are expansive[35] and interprets the definition of a VASP to include "a

central party with some measure of involvement" with a DApp.[36] This involvement could include "creating and launching an asset, setting parameters (for the operation of the DApp), holding an administrative "key" or collecting fees."[37] This broad interpretation would potentially bring a variety of DeFi participants within the definition of a VASP and subject them to compliance with anti-money laundering and counter-terrorism financing ("**AML/CFT**") laws in jurisdictions that implement this interpretation of the VASP definition.

The Updated FATF Guidance also clearly recognizes that a DApp itself is not a VASP as the standards do not apply to underlying software or technology.[38] In fact, "the FATF standards are intended to be technology neutral."[39] This position underscores the idea that code deployed to a functional blockchain network is unstoppable – it is immutable and is not something that can practically be regulated. Instead, FATF and other regulators have sought to expand the scope of existing definitions, such as VASP, in order to fill perceived regulatory gaps by bringing certain participants in DApps within the ambit of existing regulatory regimes.

The Updated FATF Guidance is also clear that it does not seek to regulate users of virtual assets as VASPs.[40] Instead, the focus is on VASPs as facilitators of certain virtual asset activities.

FinCEN "Requirements for Certain Transactions Involving Convertible Virtual Currency or Digital Assets"

In December 2020, FinCEN published a notice of proposed rulemaking regarding "Requirements for Certain Transactions Involving Convertible Virtual Currency or Digital Assets" (the "**NPRM**").[41] The stated objective of the NPRM was to aid law enforcement in the reduction of the illicit use[42] of CVC held in "unhosted wallets" or in wallets hosted in a jurisdiction identified by FinCEN. Initially, the comment period for the 72-page NPRM was 15 days. That comment period was later extended and there has not yet been a final rulemaking following the NPRM and the close of the comment period.

Despite the fact that the NPRM has not moved to final rulemaking, the NPRM was certainly designed to bring transactions in CVCs squarely within the regulatory ambit of the BSA. It would do so by imposing strict reporting and recordkeeping requirements on financial institutions, primarily aimed at centralized CVC exchanges, with respect to CVC transactions in an attempt to promote law enforcement. By requiring financial institutions to know the "[t]he name and physical address of each counterparty to the transaction of the financial institution's customer, as well as other counterparty information the Secretary may prescribe as mandatory on the reporting form for transactions subject to reporting pursuant to § 1010.316(b),"[43] the proposed rules would ostensibly allow for the identification of unhosted wallet users who choose to transact with financial institutions that would be subject to the rules.

In addition to the practical and technological compliance difficulties presented, the proposed strict recordkeeping requirements with respect to transfers of CVCs go beyond the more flexible rules currently applicable to transfers of dollars or other fiat currencies by customers of financial institutions. If the NPRM is finalized in current form, financial institutions may determine that doing business with unhosted wallets is not worth the added compliance expense. This would result in unhosted wallet activity remaining outside of financial institutions subject to the BSA and related regulations, exactly the opposite of what the NPRM is attempting to accomplish.

If finalized, these rules might also encourage users of digital assets to turn to alternatives. DeFi protocols, including "smart contract"-based P2P exchange tools, that are not owned or

controlled by any one or more identifiable persons or businesses are the likely alternative. An increase in the use of non-regulated storage solutions and P2P exchange services would cause law enforcement to lose access to information generated by centralized and regulated exchange platforms, the primary target of the NPRM and one of law enforcement's most valuable partners. CVC that remains on self-hosted wallets and transacted only in decentralized protocols is much more difficult to track and regulate absent new laws or regulations, or new interpretations of our laws and regulations. Accordingly, the struggle to regulate DeFi protocols is taking center stage.

Finally, the NPRM defines CVC broadly and does not account for the fact that CVCs are often used for purposes other than payment, such as being staked to contribute to securing a proof of stake network. To foster the use and benefits of blockchain technology and CVCs, proposed regulations that treat transactions in CVCs that are used for multiple purposes, not all of which involve payments or transfers of value, more strictly than transactions in fiat currency, which is only used for one purpose, should be re-examined.

Report of the Attorney General

A report prepared by the Cyber-Digital Task Force of the Office of the Deputy Attorney General highlighted the distinction between centralized and P2P exchanges and indicated that P2P exchanges are still subject to AML/CFT compliance:[44]

> "[U]nlike centralized virtual asset exchanges, P2P exchange platforms may operate without an intermediary that will accept and transmit virtual assets in exchange for fiat or another type of virtual asset, or that will collect customer identification information. Individual exchangers—as well as platforms and websites—that fail to collect and maintain customer or transactional data or maintain an effective AML/CFT program may be subject to civil and criminal penalties."[45]

The Cyber-Digital Task Force Report indicates that platforms or websites that fail to collect certain information may be violating the law and subject to penalties.

The Cyber-Digital Task Force Report highlights a focus on sanctions compliance with respect to digital assets. Using digital assets to hide financial transactions for the purpose of avoiding sanctions is identified as an illicit use of digital assets in the Report.[46] U.S. persons and persons otherwise subject to the jurisdiction of the Office of Foreign Assets Control of the Treasury Department "are responsible for ensuring that they do not engage in transactions prohibited by OFAC sanctions (such as dealings with blocked persons or property) or in otherwise-prohibited trade or investment-related transactions. Prohibited transactions generally also include those that evade or avoid, have the purpose of evading or avoiding, cause a violation of, or attempt to violate prohibitions imposed by OFAC under various sanctions authorities."[47]

SEC Guidance

The SEC has also sought to bring activity involving digital assets and DeFi within its regulatory ambit. The primary focus in this effort is investor protection and ensuring that this public policy goal is being achieved in the context of blockchain and digital assets. In the view of new SEC Chair Gary Gensler, "Right now, we just don't have enough investor protection in crypto. Frankly, at this time, it's more like the Wild West."[48]

In fact, the SEC was one of the first regulators to bring an action holding a developer of a decentralized exchange responsible for violating the securities laws.[49] In November of 2018, the SEC settled an enforcement action involving EtherDelta, a protocol for the P2P exchange of digital tokens that was billed as "decentralized."[50] The SEC entered into a

consent order with Zachary Coburn, an individual and the founder of EtherDelta, to resolve the investigation.[51] The order alleged that EtherDelta was an unregistered exchange because at least some of the tokens traded on EtherDelta were unregistered securities.[52] In addition, Coburn was alleged to have caused the EtherDelta "trading system" to violate certain provisions of the Exchange Act. Coburn caused these violations by: creating EtherDelta; coding and deploying the smart contract; having exclusive control over administrative keys to the EtherDelta smart contract (allowing him to change the fees charged for exchanges); and promoting EtherDelta on Twitter and Reddit.[53] The SEC deemed Coburn responsible for this P2P protocol given his significant involvement in the protocol.

A necessary element of securities law jurisdiction is activity involving an asset that meets the definition of a security. Activity that does not involve a security is not subject to the jurisdiction of the SEC. In the Coburn Order, the SEC did not specifically identify the asset(s) trading on EtherDelta that they determined were securities, and which would trigger a requirement to register as an exchange or operate within an applicable exemption from such registration.[54] In addition to the Coburn Order, the SEC has taken action against a variety of other intermediaries for failing to register as required when engaging in activities involving digital assets, or transactions in digital assets, deemed by the SEC to be securities.[55] In each of these cases, the SEC has declined to specifically identify the digital asset, or transaction in digital asset, that constituted the security triggering an obligation to register as a securities intermediary.[56]

Recent statements from newly appointed SEC Chair Gary Gensler take a similar tack, indicating a view that many tokens (digital assets) may be securities and that an exchange that facilitates the trading of lots of digital assets is probabilistically engaging in unregistered exchange activity.[57] In other words, rather than telling those engaging with digital assets when they believe specific assets are securities, the key in determining whether regulatory obligations are triggered for intermediaries pursuant to our securities laws, the regulator is instead telling those facilitating transactions in digital assets to do their own research and, if they engage in a lot of activity, they should assume that at least some of it will involve digital assets the SEC believes are securities.

At the same time, the SEC is warning digital asset market participants that they believe many digital assets should be treated as securities.[58] "Make no mistake: It doesn't matter whether it's a stock token, a stable value token backed by securities, or any other virtual product that provides synthetic exposure to underlying securities. These products are subject to the securities laws and must work within our securities regime."[59]

Chair Gensler has also addressed DeFi in recent statements as well, noting that:

> "The American public is buying, selling, and lending crypto on these trading, lending, and DeFi platforms, and there are significant gaps in investor protection.
>
> Make no mistake: To the extent that there are securities on these trading platforms, under our laws they have to register with the Commission unless they meet an exemption.
>
> Make no mistake: If a lending platform is offering securities, it also falls into SEC jurisdiction."[60]

The SEC has recognized that there are regulatory gaps when it comes to digital assets, and has expressed a desire to help fill those gaps.[61] While it remains to be seen whether the SEC will bring actions with respect to DeFi platforms, it certainly seems that they will attempt to bring as many digital assets and digital asset transactions as possible within the definition of security in order to assert jurisdiction over the issuers of those assets as well as the intermediaries facilitating transactions in those assets in order to fill any regulatory gaps.

CFTC

The CFTC has expressed similar concerns with respect to commodity derivatives activity involving digital assets occurring outside its regulatory framework. In a June 2021 speech, then Commissioner Daniel Berkovitz[62] expressed concerns about DeFi cutting out traditional intermediaries that are relied upon to provide important services, stability, and safety to our financial markets by virtue of their regulated status.[63] Eliminating those intermediaries in favor of P2P markets also eliminates the important benefits and protections that intermediaries provide to market participants.[64] Commissioner Berkovitz goes on to indicate that unlicensed DeFi markets for derivative instruments are illegal under the CEA, as those instruments are generally required to be traded on a DCM or a swap execution facility ("**SEF**").[65] He notes that DeFi markets, platforms, or websites are not registered as DCMs or SEFs and that there is no exception from registration for smart contracts or digital assets.[66] Accordingly, we may see increased regulatory scrutiny of blockchain-based systems that facilitate transactions in digital assets that could be deemed commodity derivatives.

Responses from DeFi

Aave and Compound Finance are two of the DeFi industry's best-known permissionless liquidity protocols. Aave is an open-source and non-custodial liquidity protocol for earning interest on deposits and borrowing assets,[67] while Compound is an algorithmic, autonomous interest rate protocol built for developers in order to unlock a universe of open financial applications.[68] Fundamentally, both protocols allow individuals to lend or borrow digital assets with lenders, or liquidity providers, earning interest on the assets they provide or paying interest on assets borrowed. The returns generated by DeFi protocols like Aave and Compound have sparked institutional interest, but financial institutions need to comply with AML, know-your-customer ("**KYC**"), and know-your-transaction rules and regulations. To address this, both Aave and Compound Finance have launched permissioned versions of their protocols to allow institutional participation in a controlled environment with known participants.

Aave Arc

Aave Arc is a new, permissioned protocol being designed by Aave specifically for institutional investors.[69] By completing a required KYC process, large corporations and financial clients will be able to utilize the Aave protocol while also complying with applicable laws and regulations.[70] In order to ensure compliance, these permissioned pools will be separated from Aave's other deployments, and be inaccessible to non-qualified participants.[71] Furthermore, Aave Arc will include a "whitelisting layer" onto its smart contracts to ensure that only those institutions that have successfully completed the KYC verification can access the permissioned protocol.[72] Initially, only four assets – Bitcoin, Ether, Aave, and USDC – will be supported by the protocol.[73]

With the exception of the KYC requirement and the whitelisting or blacklisting by Fireblocks, effectively acting as gatekeepers, Aave Arc seems to mimic the experience offered by Aave, the permissionless version of the protocol. The distinction, of course, is security – liquidity providers are known and traceable, as opposed to the pseudonymous users of Aave. Another distinction is that only four assets will initially be available in these segregated pools.

Compound Treasury

Compound Labs, creators of the Compound Finance protocol, launched a similar protocol called Compound Treasury at the end of June 2021.[74] In addition to compliance, Treasury was designed to make the customer experience simple by removing protocol complexity

such as private key management, crypto-to-fiat conversion, and interest rate volatility.[75] Businesses can wire U.S. dollars to their Compound Treasury Account, which will then be converted into USDC and deployed onto the protocol. They will be able to earn a guaranteed fixed rate of interest on such deployed assets and are free to withdraw their funds at any time.[76] Like Aave Arc, this product is permissioned such that institutions will have to register in order to use the protocol.[77]

Treasury users seemingly never directly interact with the protocol. Instead, they simply provide fiat, which is then converted to USDC stablecoins and deployed onto the platform. Compound Finance, the permissionless protocol, allows users to directly contribute ERC-20 tokens to liquidity pools and users are constantly chasing pools with the highest returns, a tactic known as yield farming. By limiting the investment to USDC stablecoins and guaranteeing a return, most of the risk is removed.[78] Treasury "users" have a much different experience than the users of Compound Finance.

These permissioned protocols designed to provide institutional access to quasi-DeFi show that developers can build KYC into these protocols when desired. The idea of KYC is in conflict with the concept of DeFi, which is built on an ethos that values privacy and enabling composable P2P pseudonymous transactions. However, these permissioned protocols are likely a recognition of the fact that regulated institutional market participants can only engage with protocols that have the compliance features necessary to allow them to meet their regulatory obligations. They signal a new direction for DeFi in which certain aspects of DeFi protocols are made available on a permissioned basis in order to foster regulatory compliance and truly open and permissionless DeFi protocols continue to exist as unstoppable code.

DeFi and permissioning

A dual regulatory system that allows open access to DeFi's "unstoppable code" for those individuals and businesses that have the means and ability to use these protocols, complemented by permissioned access points to these protocols for others, could have significant benefits.[79] Such an approach would allow for regulated access to rapid technological developments occurring in the DeFi space. It would also acknowledge the reality that, as long as access to the Internet is available, the blockchain-based smart contract code underlying these protocols will be accessible to anyone with the necessary technical ability on a permissionless and anonymous basis. Regulators should seize this opportunity to work with DeFi participants to encourage ongoing innovation and to strike a balance between preserving the autonomous nature and spirit of DeFi while also establishing regulated access points to these protocols, where appropriate (for example, for commercial grade transactions or by fiduciaries acting on behalf of third parties). These permissioned access points can serve as regulated intermediaries responsible for compliance with securities, commodities, or financial regulatory laws, as applicable, depending on the type of assets transacted using the protocol.

In such a dual-track system, regulators would have less of a need to expand intermediary definitions to fill regulatory gaps. For instance, we would not need to treat digital assets as securities to bring secondary transactions within our securities law regulatory framework. This would be more consistent with the application of the *Howey* test to determine when a digital asset is initially sold in an investment contract scheme.[80] The *Howey* test is a facts-and-circumstances-dependent test that has been applied in the context of initial sales and requires a variety of elements to be present in order for a particular scheme to be deemed an investment contract.[81] However, when a digital asset initially sold in an investment contract

is resold in a secondary transaction, the *Howey* test is difficult to apply and more difficult still to satisfy. The object of the initial investment scheme is very rarely a security in and of itself. This may be why, in all the actions taken to date against intermediaries whose securities law obligations are only triggered by secondary transactions in digital assets, the particular assets believed to be securities have not been identified.[82]

Rather than continuing down this path of confusion with respect to both centralized and decentralized platforms, establishing regulated access points to DeFi protocols could bring a portion of the related activity with respect to these assets within the regulatory perimeter from both a KYC/AML perspective and from the perspective of protecting those that transact using these permissioned access points. The U.S. also maintains robust federal- and state-level consumer protection laws that have been flexibly applied to address a wide variety of consumer issues, from deceptive marketing of drugs to unfair and deceptive practices with respect to residential mortgage-backed securities to deceptive statements in connection with credit ratings. Consumer protection frameworks in the U.S. provide ample regulatory authority to protect purchasers of digital assets that can be used to access blockchain-based services, contribute to the security of blockchain networks, or transfer value.

Regulation of permissioned access points from a financial regulatory and consumer protection perspective can be greatly enhanced by leveraging rich and highly granular data availability associated with blockchain ledgers – much more than is available in the world of traditional finance. Rather than relying on the after-the-fact oversight conducted in traditional finance, regulators engaging with DeFi (both permissioned and open access) can tap into the vast pools of real-time data generated by blockchain networks. Coupling this data with blockchain analytics means that regulators have an unprecedented ability to monitor transactions and information, which may be helpful with respect to identifying concerning activity in both permissioned and open DeFi protocols. Utilizing these tools to monitor transaction activity may provide the foundation for a new regulatory approach to blockchain-based transactions that does not necessarily rely on inefficient manual oversight of, or highly fallible self-reporting by, regulated intermediaries. This would be especially valuable with respect to those choosing to use open access DeFi protocols, while permissioned access points could be regulated as intermediaries, combining traditional and blockchain-based oversight.

This dual system could allow for DeFi to continue to grow and develop for the benefit of the future of finance. Regulators should work with DeFi builders and market participants towards an optimal regulatory solution that allows for continued growth and innovation, while providing meaningful protections to all stakeholders.

* * *

Endnotes

1. https://defipulse.com/.
2. 15 U.S.C. § 77j.
3. 15 U.S.C. § 78j.
4. 15 U.S.C. §§ 77e(a) and (c).
5. 15 U.S.C. § 77d. Exemptions from registration include Regulation D, Regulation A, Regulation CF, and the intrastate offering exemption.
6. 15 U.S.C. § 78l.
7. For example, broker-dealers must register with the SEC pursuant to 15 U.S.C. § 78o.

8. 7 U.S.C. § 1.
9. *See*, *e.g.*, https://www.cftc.gov/IndustryOversight/Intermediaries/index.htm.
10. *See*, *e.g.*, CEA § 4(a).
11. Transactions in commodity derivatives by eligible contract participants are not required to take place on a DCM. Eligible contract participants are generally highly sophisticated and well-capitalized entities or individuals. *See* 7 U.S.C. § 1a(18). Retail market participants may also be referred to as non-eligible contract participants.
12. "Financial institution" is a broad category of business offering financial services. 31 U.S.C. § 5321(a).
13. 31 U.S.C. § 5330 and 31 C.F.R. § 1022.380(b)(2).
14. 31 U.S.C. §§ 5318(a)(2) and (h); 31 C.F.R. § 1022.210(a).
15. 31 U.S.C. §§ 5318(a)(2) and (h)(1); 31 C.F.R. §§ 1022.210(c) and (d).
16. 31 C.F.R. § 1010.100(ddd).
17. 31 C.F.R. § 1010.410(f).
18. *Id*.
19. *Id*.
20. 31 C.F.R. §§ 1010.410(e) (funds transfer recordkeeping for BSA financial institutions and other banks) and 1010.410(f) (the Travel Rule).
21. *See* Application of FinCEN's Regulations to Certain Business Models Involving Convertible Virtual Currencies (https://www.fincen.gov/sites/default/files/2019-05/FinCEN%20Guidance%20CVC%20FINAL%20508.pdf). FinCEN first addressed rule-making authority over virtual currency in March 2013, clarifying that it would regulate transmitters of virtual currency in the same manner as transmitters of fiat currency. Application of FinCEN's Regulations to Persons Administering, Exchanging, or Using Virtual Currencies, FIN-2013-G001 (Mar. 18, 2013) (the "**2013 Guidance**"). Since issuing the 2013 Guidance, FinCEN has issued other Guidance and rulings on virtual currency that further inform the application of existing money transmission regulations: Application of FinCEN's Regulations to Virtual Currency Software Development and Certain Investment Activity, FIN-2014-R002 (Jan. 30, 2014) (the "**2014 Software and Investment Guidance**"); Application of FinCEN's Regulations to Virtual Currency Mining Operations, FIN-2014-R001 (Jan. 30, 2014) (the "**2014 Mining Guidance**"); and Request for Administrative Ruling on the Application of FinCEN's Regulations to a Virtual Currency Payment System, FIN-2014-R012 (Oct. 27, 2014) (the "**2014 Payment System Ruling**").
22. *Id*.
23. *Id*.
24. *Id*.
25. *Id*.
26. *Id*.
27. *Id*.
28. *Id*.
29. *See Recommendation 15*, Financial Action Task Force.
30. *See Interpretive Note to Recommendation 15* (INR. 15), Financial Action Task Force (June 2019).
31. *See Interpretive Note to Recommendation 15* (INR. 15), Financial Action Task Force (June 2019).
32. *See Interpretive Note to Recommendation 15* (INR. 15), Financial Action Task Force (June 2019).

33. *See Draft Updated Guidance for a Risk-Based Approach to Virtual Assets and VASPs*, Financial Action Task Force (March 2021).
34. *Id*. at paragraph 47.
35. *Id*. at paragraph 76.
36. *Id*. at paragraph 56.
37. *Id*.
38. *Id*. at paragraph 57.
39. *Id*. at paragraph 68.
40. *Id*. at paragraph 70.
41. *See* "*Requirements for Certain Transactions Involving Convertible Virtual Currency or Digital Assets*," Financial Crimes Enforcement Network, 85 FR 83840 (Dec. 23, 2020), available at: https://www.federalregister.gov/documents/2020/12/23/2020-28437/requirements-for-certain-transactions-involving-convertible-virtual-currency-or-digital-assets.
42. The term "illicit use," for purposes of this chapter, refers to any unlawful use of CVCs or other monetary instruments, including for money laundering, terrorist finance, ransomware or other criminal activity.
43. Proposed 31 C.F.R. § 1010.410(g)(1)(vii).
44. *See* "*Report of the Attorney General's Cyber-Digital Task Force*" (the "**Cyber-Digital Task Force Report**"), available at: https://www.justice.gov/ag/page/file/1326061/download.
45. Cyber-Digital Task Force Report at p. 38. Where the exchange platform is a decentralized computer protocol rather than a business or individual, there may be no one to collect information or to maintain transaction records, nor anyone to prosecute for not doing so.
46. *Id*. at 26.
47. *Id*. at 26.
48. *Remarks Before the Aspen Security Forum* (the "**Aspen Speech**"), SEC Chair Gary Gensler (Aug. 3, 2021).
49. *In the Matter of Zachary Coburn* (Securities Exchange Act Rel. No. 84553) (Nov. 8, 2018) (the "**Coburn Order**").
50. *Id*.
51. *Id*.
52. *Id*.
53. *Id*.
54. *Id*.
55. *See*, *e.g.*, the Coburn Order; *In the Matter of TokenLot, LLC, Lenny Kugel, and Eli L. Lewitt* (Securities Act Rel. No. 10543, Exchange Act Rel. No. 84075, Investment Company Act Rel. No. 33221) (Sept. 11, 2018); *In the Matter of ICO Rating* (Securities Act Rel. No. 10673) (Aug. 20, 2019); *In the Matter of Blotics LTD. f/d/b/a Coinschedule LTD.* (Securities Act Rel. No. 109546) (July 14, 2021); *In the Matter of Poloniex* (Exchange Act Rel. No. 92607) (Aug. 9, 2021).
56. The only SEC enforcement actions with respect to digital assets in which they allege a digital asset is a security are those actions against "issuers" for failure to register a specific asset as a security. In contrast to those matters, the enforcement actions against intermediaries for failure to register do not identify the digital assets that the SEC believes are securities and that trigger the registration obligation.
57. *See* the Aspen Speech, *supra* note 48.
58. *Id*.
59. *Id*.

60. *Id*.
61. *Id*.
62. *Keynote Address of Commissioner Dan M. Berkovitz Before FIA and SIFMA-AMG*, *Asset Management Derivatives Forum 2021* (the "**FIA Speech**"), CFTC Commissioner Dan M. Berkovitz (June 8, 2021).
63. *Id*.
64. *Id*.
65. *Id*.
66. *Id*.
67. https://aave.com.
68. https://compound.finance.
69. Kofi Ansah, *Aave Set to Unveil Permissioned DeFi for Financial Institutions in July*, Coinspeaker (July 5, 2021), https://www.coinspeaker.com/aave-permissioned-defi-institutions/.
70. Sarah Tran, *Aave Pro to Launch in July for Institutional Access to DeFi Markets*, FXStreet (July 6, 2021), https://www.fxstreet.com/cryptocurrencies/news/aave-pro-to-launch-in-july-for-institutional-access-to-defi-markets-202107060509.
71. Ansah, *supra* note 3.
72. Ansah, *supra* note 3.
73. Sean Dickens, *Aave to Debut Institutional DeFi Lending via Aave Pro*, Yahoo!: News (July 7, 2021), https://news.yahoo.com/aave-debut-institutional-defi-lending-154914554.html.
74. https://compound.finance/treasury.
75. Calvin Liu, *Announcing Compound Treasury, for Businesses & Institutions*, Medium (June 28, 2021), https://medium.com/compound-finance/announcing-compound-treasury-for-businesses-institutions-83d4484fb82e.
76. Aisshwarya Tiwari, *Compound (COMP) Unveils Institutional-Grade DeFi Product Compound Treasury*, BTCManager (June 29, 2021), https://medium.com/compound-finance/announcing-compound-treasury-for-businesses-institutions-83d4484fb82e.
77. Sergio Goschenko, *Compound Launches Treasury to Introduce Institutions to DeFi*, Bitcoin.Com: News (July 7, 2021), https://news.bitcoin.com/compound-launches-treasury-to-introduce-institutions-to-defi/.
78. Brady Dale, *Compound Labs Launches "Treasury" to Get Big Firms Reaping DeFi Yields*, CoinDesk (June 28, 2021), https://www.coindesk.com/compound-labs-launches-treasury-to-get-big-firms-reaping-defi-yields.
79. *See* Alex Lipton and Lewis Cohen, "*DeFi: a pathway forward*," IFLR (Sept. 9, 2021), https://www.iflr.com/article/b1thnhzpsrjkqf/defi-a-pathway-forward.
80. *SEC v. W.J. Howey Co.*, 328 U.S. 293 (1946).
81. *Id*.
82. *Supra*, note 55.

Lewis Cohen
Tel: +1 202 754 2012 / Email: lewis.cohen@dlxlaw.com

Lewis provides in-depth legal counsel to startups, major enterprises, and governmental entities on a broad range of matters involving the use of blockchain, cryptocurrencies and other disruptive technologies. He is passionate about the ability of innovative technologies to change the way businesses and individuals work together, and is a major advocate for the potential of emerging technologies to benefit and transform industries around the globe. Lewis has more than 20 years of experience in traditional capital markets and finance and is a frequent public speaker on the topic of blockchain and distributed ledger technology. Lewis is also recognized by *Chambers Global* as one of only three lawyers in "Band 1" for Legal: Blockchain & Cryptocurrencies – USA.

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, where she was recognized by *The Legal 500 US* among the top finance attorneys in the U.S.

Greg Strong
Tel: +1 302 766 5535 / Email: greg.strong@dlxlaw.com

Greg advises clients on compliance with securities laws, commodities laws, and other laws and regulations that may apply to activities involving blockchain and digital assets. He has successfully represented clients before the Securities and Exchange Commission, and various other regulators. In addition, he has worked on a variety of cutting-edge transactions involving digital assets.

Prior to joining DLx Law, Greg was a Deputy Attorney General in the Delaware Department of Justice from 2003 to 2018. During that time, Greg served as the Director of Investor Protection for the State of Delaware for three years and was responsible for administering and enforcing Delaware securities laws. Greg also served as the Director of the Consumer Protection Unit for three years.

DLx Law

4913 43rd St. NW, Washington, D.C. 20016 / 114 East 25th Street, New York, NY 10010 /
1007 N. Orange Street, Wilmington, DE 19801, USA
Tel: +1 212 994 6845 / URL: www.dlxlaw.com

Legal considerations in the minting, marketing and selling of NFTs

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

The increased popularity of people consuming and collecting content in digital form in recent years 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. While market numbers vary, the NFT market is expected to be well over a $2 billion market in 2021. 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 a pointer to an off-chain location where the work associated with the NFT is stored.[1]

Although we are in the nascent stages of how creators, rights holders and brands might exploit NFTs, there have already been significant developments in a number of different sectors. For example, rights holders, including entertainment companies and sports leagues, are using NFTs as a way to create and market digital collectibles both for existing and potentially new fans. Video gaming companies are looking at ways NFTs can be implemented to allow users to purchase, trade, and rent out in-game assets. In the music industry, NFTs are being used by artists to connect directly with fans as well as generate new

sources of revenue. For example, the band Kings of Leon made headlines when it released an album that also had an NFT version. Those who purchased the album through the NFT also received enhanced visual media, a digital download of the music, and a limited-edition vinyl. The band also auctioned off a second type of NFT that included four front row tickets to one Kings of Leon headline show per tour anywhere in the world, a meet and greet with the band, tour merchandise, and use of an SUV limousine. As the Kings of Leon example demonstrates, NFTs can also serve as a type of digital identifier that allows an individual to claim a physical asset or service. In the art world, the most famous NFT sale was a Christie's auction of an NFT attached to a digital collage by the artist known as "Beeple," which went for $69 million. However, in addition to the high-end auction world, digital artists are using NFTs as a way to monetize their original, creative works.

Finally, there is a growing market for so-called "community NFTs." This is when a series of NFTs of a certain type of character are minted (e.g., animated pandas, apes, cats, etc.) each of which is slightly different (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 and unlock certain user experiences.

Key stakeholders in the NFT market

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

- *Platform Providers*. A number of NFTs are designed to operate, and are stored on, the Ethereum blockchain. However, numerous other blockchains exist and some are being developed with a focus on the sending, receiving and storing of NFTs.
- *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, etc.). 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).[2]

Technology background

In order to understand the legal issues raised by NFTs, it is important to understand some of the technology underpinnings. Markets typically rely on a trusted third party to authenticate market participants and maintain a central ledger of each party's holdings. Blockchain technology, which underpins most cryptocurrencies, seeks to replace that trusted third party with a fully decentralized network of computers storing an identical copy of the ledger and validating blocks of new transactions through a consensus-based mechanism. Participants are not authenticated by a central third party, but through a method of cryptography known as "private-public key encryption." A powerful feature of blockchains, and one that is essential to NFTs, is that because each block of transactions is cryptographically based on the previous block, they are immutable; meaning that for all practical purposes, historical records cannot be altered or deleted. 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).

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. 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 have moved to the forefront of discussions around blockchains in 2021, 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.

A key market feature of an NFT results from the fact that it is a programmable piece of computer code. This allows developers to include a programmable royalty (or resale) function that automatically transfers a specified amount of cryptocurrency 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 a blockchain. This technology opens up numerous new opportunities to reward those involved in an NFT project and, most importantly, allows creators and rights holders to directly benefit from the increased value of an NFT as it is resold. While such payment schemes are being rolled out, many NFT marketplaces have implemented incompatible approaches to royalties, creating uncertainty as to whether royalties will be honored as NFTs are transferred across platforms. A royalty payment standard (EIP-2981) that would standardize royalties, at least for ERC-721 tokens, is currently in development. Still, standardization has its limits since the standard adopted for one blockchain may not be compatible with that adopted for another.

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. In effect, who has the right to grant a purchaser with a digital "certificate of ownership" of an "authentic" version. Given that NFTs have only recently been adopted as a means of identifying digital goods, it comes as no surprise that most 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 are being added to many such agreements (as discussed below), for the time being, 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.

One of the most interesting intellectual property questions presented by NFTs is what copyright rights are necessary to "tokenize" a digital work as an NFT. 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.[3] This "bundle of

rights" can be held or licensed by the copyright holder in whole or in part, but critically, unless the rights are expressly assigned or licensed away, they remain with the author of the work.

Further complicating matters is that the creator of a work is not necessarily the copyright owner. The creator, or in copyright parlance, "author," of a work may not necessarily be the holder of the copyright in that work or have sufficient rights to tokenize that work into an NFT. 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.[4] In all other cases, the author must explicitly assign their copyright in a work for it to transfer. The nuance between whether the copyright in a work initially vested in a party or was assigned to it can have important repercussions. In general, assignors of a copyright have a "right of reversion" under which they can terminate the assignment and reclaim their copyright after 35 years.[5] While this may seem like a distant problem, purchasers of NFTs as collectibles or for long-term investment purposes may want to know whether the original author has a right of reversion.

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 that 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 or musical artist that does not own the copyright in a piece of music wants to create a derivative work of a composition or a master recording, such as 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."

Given the foregoing, where does this leave 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 amongst multiple parties, including through exclusive license arrangements, the answer may be less clear. The minting of an NFT requires at least some exercise of copyright rights since the work needs to be displayed, 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 it on all future technologies to be developed. Whether these clauses include the right to mint NFTs will require a case-by-case analysis, although courts have interpreted these clauses to include new technologies.[6]

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 is jurisdiction-specific but generally

protects 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 they may include an author's control over whether and in what way their work is displayed and how it is used.[7] 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 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.

Other rights to consider

While copyright issues are the ones that predominate to date in the NFT sectors, 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.[8] 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 prohibited.[9] 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.

Incorporating an individual's NIL into an NFT without authorization risks infringement of that individual's right of publicity. The right of publicity is an intellectual property 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.

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 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 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 instead on content identification, 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 a creator modified its 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 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 company that goes out of business, that work could be lost.[10]

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, this important technical point 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 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 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.

As a general matter, any right to commercialize the work is expressly carved out, or is 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.

The typical NFT terms of use also set forth certain restrictions on how the creative work underlying the NFT may be used. For example, a number of license agreements, including the NFT License 2.0, 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.[11] 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.[12] 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.[13] 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.[14] 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.

One issue that has not yet been resolved is the applicability of license terms to downstream purchasers. To the extent a purchaser is buying an NFT on the same marketplace where it was first sold, there should not be any issue since 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. 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.

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. For example, DC Comics cautioned its freelancers in a letter that was leaked that the offering for sale of any digital images that include DC's intellectual property with or without NFTs is not permitted.[15]

If an NFT is minted without the authority of the rights holder, they likely have 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. Rights holders may have the most success focusing on the centralized touch points of this 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.[16] However, a successful take-down likely only means the images of the work displayed on the marketplace will be removed. It does not mean that the infringing work is being deleted from whatever platform it may be stored on, and the rights holder would need to pursue those rights separately. 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 requesting certain identifying information about the infringer.[17] 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 itself 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.[18] Given the active role that many marketplaces play in the minting and offering of NFTs, the second prong could be easy to establish.[19] 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.[20]

Remedies for NFT purchasers

In the event that a work associated with an NFT is taken down due to copyright infringement or otherwise, the rights of the NFT owner may be significantly limited. As an initial matter, locating the person or entity that minted the infringing NFT may be difficult, given the fact that the blockchain only includes alphanumeric public keys of blockchain participants and the fact that 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, they will disclaim any liability for the NFTs themselves; an important point since NFTs are basically pieces of computer code residing on a blockchain.

The terms of service 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 as is, 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 volatility of blockchain and digital assets;
- 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; 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, and are paid for in cryptocurrencies and can be effectuated 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.

Anti-money laundering considerations

While the U.S. Department of the Treasury's Financial Crimes Enforcement Network (FinCEN)[21] has not yet indicated whether certain NFT market participants (e.g., creators, sellers, dealers, marketplace operators) are or may become subject to U.S. anti-money laundering (AML) regulatory requirements, recent developments and concerns of U.S. lawmakers and regulators regarding the financial crime risks associated with virtual assets make regulatory scrutiny of NFTs likely.

In March 2021, the Financial Action Task Force (FATF) – an intergovernmental organization that develops standards to combat money laundering and terrorism financing – issued draft updated virtual asset guidance,[22] which could have potential implications for the regulation 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 draft guidance, FATF replaced a previous reference to "assets that are fungible" with "assets that are convertible and interchangeable," in defining the scope of virtual assets that in FATF's view warrant regulation. FATF further stated that "[f]lexibility is particularly relevant in the context of [virtual assets] and [virtual asset] activities" and that "some items – or tokens – that on their face do not appear to constitute [virtual assets] may in fact be [virtual assets] that enable the transfer or exchange of value or facilitate [money laundering or terrorism financing]." FATF's latest stance may represent an effort to pave the way for the regulation of certain NFTs that have currency attributes or function as stored value.

Similarly, U.S. AML legislation passed earlier this year provides regulators flexibility and wide latitude to regulate a quickly evolving virtual asset industry. In particular, the Anti-Money Laundering Act of 2020 (AMLA) expanded the definitions of "money transmitting business" and "financial institution" under the Bank Secrecy Act (BSA) to include businesses involved in the exchange or transmission of "value that substitutes for currency."[23] While this amendment aligns with the existing position regarding virtual currencies taken by FinCEN, Congress's expansion of these definitions provides FinCEN with additional statutory authority to regulate not only existing virtual currencies, but also other emerging payment methods or novel asset classes. To date, FinCEN has not issued

any guidance or rules specifically on NFTs. However, given the wave of interest in NFTs, the high value of recent NFT sales and AML-related risk factors, we anticipate that NFTs will attract U.S. regulatory scrutiny.

Could NFTs be treated like virtual currencies?

While the regulatory classification of NFTs is sure to be the subject of much discussion, to the extent that FinCEN were to treat a particular NFT or certain types of NFTs as "value that substitutes for currency," FinCEN could potentially seek to regulate such activity under its money transmission regime. However, given that NFTs may not readily be classified as a currency substitute as in the case of convertible virtual currencies, FinCEN's determination to classify an NFT as such may depend on the specific characteristics of the NFT, how it is used, and the apparent money laundering risks involved.

In the United States, persons that accept currency, funds, or other "value that substitutes for currency" from one person and transmit it to another location or person by any means fall within the federal definition of "money transmitter." FinCEN has made clear in its guidance that virtual currency "has an equivalent value in real currency or acts as a substitute for real currency" and that "[a]ccepting and transmitting anything of value that substitutes for currency makes a person a money transmitter." In its May 2019 virtual currency guidance, FinCEN expressed a broad view of money transmission and advised that "if assets that other regulatory frameworks define as commodities, securities, or futures contracts were to be specifically issued or later repurposed to serve as a currency substitute, then the asset itself could be a type of value that substitutes for currency, the transfer of which could constitute money transmission."

A money transmitter is a type of money services business (MSB). MSBs are required to register with FinCEN and must comply with extensive requirements under the 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 regarding money laundering and sanctions evasion risks in the art trade could have potential implications for persons that deal in certain NFTs, to the extent that 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 sanctions violations.

Although participants in the art trade currently are not subject to the BSA, recent legislative developments suggest that this may change in the near future. Specifically, as part of the AMLA, Congress commissioned the secretary of the Treasury to perform a study of how trade in artwork facilitates money laundering and the financing of terrorism and to report its findings to Congress by January 1, 2022. The AMLA's extension of the BSA to "persons engaged in the trade in antiquities" might be a bellwether of forthcoming change in AML regulation of the art trade. While it is too early to say whether traders of artwork may become subject to AML regulatory requirements, any such expansion of the BSA could capture traders of digital art or similar items on the blockchain.

Securities law considerations

The programmability of NFTs also allows the creator to easily fractionalize ownership of the NFT amongst multiple parties. One aim of fractionalized 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 asset constitutes 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 asset may fall outside the "investment contract" definition when it 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 NFTs that represent rights to digital collectibles and artwork, there are strong grounds to conclude that such digital assets 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 beyond whether an NFT itself is a security to all of the facts and circumstances surrounding its 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. Thus, even where an NFT is not a security, 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.

Ultimately, while NFTs themselves are not likely to be classified as securities, further securities-related questions may hinge on the specific facts and circumstances surrounding their creation, promotion and sale.

* * *

Endnotes

1. As discussed further below, the digital work associated with an NFT is typically not stored on a blockchain.
2. 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.
3. 17 U.S.C. § 106.
4. 17 U.S.C. § 101.
5. 17 U.S.C. § 203. The right of reversion works differently depending on whether the work was created before or after January 1, 1978 when the current Copyright Act went into effect.
6. *See*, *e.g.*, *Rooney v. Columbia Pictures Indus., Inc.*, 538 F. Supp. 211, 223 (S.D.N.Y.), aff'd, 714 F.2d 117 (2d Cir. 1982).
7. 17 U.S.C. § 106A.
8. *See*, *e.g.*, 15 U.S.C. § 1114.
9. *See*, *e.g.*, *id.* at § 1125.
10. The Filecoin protocol, which complements IPFS, seeks to address this situation by rewarding nodes on the network that maintain redundant copies of files.
11. 17 U.S.C. § 109(a).
12. *Quality King Distributors, Inc. v. L'anza Research Intern., Inc.*, 523 U.S. 135, 152 (1998).
13. *Capitol Records, LLC v. ReDigi Inc*. No. 16-2321 (2d Cir. Dec. 12, 2018).
14. 17 U.S.C. § 109; *Apple Inc. v. Psystar Corp.*, 658 F.3d 1150, 1155 (9th Cir. 2011).
15. "DC Comics Warns Freelancers Not to Participate in NFT Auctions Featuring the Company's IP," (Mar. 15, 2021) available at https://news.bitcoin.com/dc-comics-warns-freelancers-nft-auctions-featuring-companys-ip/.

16. Under Section 512 of the Copyright Act, "provider[s] 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.
17. 17 U.S.C. § 512(h).
18. *See*, *e.g.*, *A&M Records, Inc. v. Napster, Inc.*, 239 F.3d 1004, 1019 (9th Cir. 2001).
19. 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.
20. *Perfect 10 v. Amazon.com, Inc.*, 508 F.3d 1146, 1171 (9th Cir. 2007).
21. 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.
22. FATF, Public Consultation on FATF Draft Guidance on a Risk-Based Approach to Virtual Assets and Virtual Asset Service Providers (March 2021).
23. *See* our January 2021 client alert "US Enacts Historic Legislation To Strengthen Anti-Money Laundering and Counterterrorist Financing Legal Framework" for additional discussion of this legislation.

* * *

Acknowledgments

The authors are grateful for the contributions of Skadden associates Mana Ghaemmaghami, MacKinzie Neal, Vartan Shadarevian, and Javier Urbina to this chapter, and Skadden summer intern Camille Brown.

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. His background in computer science and the information technology industry allows Mr. Levi to understand the technology and business drivers underlying transactions and agreements in these areas.

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's blockchain- and virtual currency-related representations include a developer of a stablecoin platform and virtual currency, a developer of a new blockchain platform and related virtual currency, a global bank in connection with its implementation of a distributed ledger platform and a developer of a decentralized virtual currency exchange. 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; representing individuals and companies in numerous SEC investigations and enforcement actions relating to the offer and sale of digital assets; advising transportation network companies in connection with the ride-hail industry, including litigation challenging administrative rulemaking and regulations; and obtaining numerous dismissals of securities class actions and shareholder derivative lawsuits involving alleged violations of federal securities laws.

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 identified and discussed already 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.

In the last couple of years, a significant number of VAs have emerged and at least some of them attracted significant investment in payment infrastructures built on the relevant software protocols. These payment infrastructures 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 2020 that illicit activity represented 0.34% of cryptocurrency volume, down from 2.1% in 2019.[3]

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 October 2018, FATF adopted changes to its Recommendations 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.

More recently, FATF released its Draft Updated Guidance for a Risk-Based Approach to Virtual Assets and Virtual Asset Service Providers (the "**Updated Guidance**"), which is an update to the guidance released in 2019. The final Updated Guidance is expected to be released by November 2021. If adopted by FATF, the Updated Guidance will constitute 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.

Finally, FATF updated its Recommendations in October 2018 and introduced the definition of VAs, now defined as a "*digital 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] 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.[7] In addition, the Updated Guidance states that entities involved in stablecoin arrangements may have AML/CFT obligations, 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.

For the purposes of this chapter, we will adopt the definitions and conceptual framework set out in FATF's updated Recommendations.[8] 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 US 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 by each jurisdiction at the level of financial intermediaries 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 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 AML/CFT 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, AML/CFT risks are heightened among the unregulated sectors of 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,[9] 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, FATF", 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, decentralised or distributed applications ("**DApps**"), VA escrow services, kiosk providers, but also entities involved with non-fungible tokens, DeFi protocols, P2P platforms as well as 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.[10]

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 toward 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 and wallet services; (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".[11]

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,[12] 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

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"[13] 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,[14] 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 will be 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 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, the European Commission adopted a digital finance package on September, 24 2020, which includes digital finance and retail payments strategies as well as four concrete legislative proposals on VAs and digital resilience. Most notably, the Proposal for a Regulation of the European Parliament and of the Council on Markets in Crypto-assets and amending Directive (EU) 2019/1937, also known as the MiCA Proposal, which would apply to all VAs not currently covered under existing financial services legislation, establishes uniform European rules for issuers of such VAs as well as for crypto-asset service providers ("**CASPs**", which have a wider scope of services than FATF's VASPs). At this stage, there is no specific timeline for MiCA's implementation, but the European Commission's expectation is that a comprehensive framework should be put in place by 2024.

Finally, 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. Most notably, the proposed reform will extend AML/CFT rules to the entire crypto sector, by narrowing the "travel rule" gap through a revision of Regulation 2015/847/EU, thereby obliging all CASPs to conduct due diligence on their customers. The legislative package is to be discussed by the European Parliament and Council, and the European Commission is hopeful for a speedy legislative process.

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,[15] 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.

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.

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.[16] 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, taking also 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).[17] 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 owners or operators of DApps are likely VASPs because they conduct exchanges or transfers on behalf of their customers, "even if other parties play a role in the service or portions of the process are automated". 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.

The Updated Guidance also affirms that P2P transactions are not subject to FATF AML/CFT obligations because FATF generally places obligations "on intermediaries between individuals and the financial system, rather than on individuals themselves with some exceptions". 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 obligation would be imposed. Further, sanctions screening and certain due diligence measures have also been introduced on VA transactions.

FATF expects to finalise and publish the final Guidance by November 2021.

(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.

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, the 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.

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 central bank cryptocurrencies ("**CBCCs**") closely or even contemplating issuing their own CBCC 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.

CBCCs 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 the BIS indicated in its March 2018 report, *Central bank digital currencies*, that the issuance of CBCCs 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 CBCCs 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 CBCC, 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. 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, 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 Chainalysis 2021 Crypto Crime Report*, January 2021.
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. 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.
8. Available here: http://www.fatf-gafi.org/media/fatf/documents/reports/Virtual-currency-key-definitions-and-potential-aml-cft-risks.pdf.
9. 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**").
10. FATF, *Virtual Currencies: Key Definitions and Potential AML/CFT Risks*, June 2014.
11. Report of the ECB on Virtual Currency Schemes, October 2012.
12. 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.
13. 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.
14. European Commission, *Explanatory Memorandum*, Proposal for a Directive of the European Parliament and of the Council amending MLD4.
15. Swiss Federal Council Report on Virtual Currencies, June 25, 2014.
16. FINMA Guidance 02/2019 – Payments on the blockchain, August 26, 2019.
17. Available here: https://www.fatf-gafi.org/publications/fatfrecommendations/documents/public-consultation-guidance-vasp.html.

* * *

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 "impressive expertise in the Fintech space" (*Who's Who Legal*, 2019) and "his great understating 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 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

Distributed ledger technology as a tool for streamlining transactions

Douglas Landy, James Kong & Ben Elron
White & Case LLP

Introduction

This chapter will provide a high-level overview of the potential applicability of distributed ledger technology ("DLT") to the transfer of assets represented by "tokens" or other digital assets[1] (which, for the purposes of this chapter, we will call "Transfer Tokens"), and the regulatory environment developing around such tokens. Using a token as a means of representing an underlying asset (colloquially referred to as the "tokenization" of that asset) in order to facilitate transfers of that asset is a relatively new idea, but has its roots in a very old and well-understood principle: some things that have value are not easily transferred. Whether due to practical difficulties, regulatory hurdles or imperfect or outdated trading infrastructures, sometimes the easiest way to transfer an asset – whether it be title, an ownership interest, an entitlement, or a beneficial interest in that asset – is by transferring something that represents the asset.[2]

Tokenization has potentially wide applicability to traditional markets. The trading of securities in the United States, for example, is beset with inefficiencies related to existing trading infrastructures. For example, purchase and sales of securities generally involve transfers of ownership that are recorded on the books of a clearing bank or the Fedwire Securities Service. Recording these transfers takes time and relies on a central intermediary. Using Transfer Tokens to represent the underlying securities can potentially streamline this process, as parties could instead exchange Transfer Tokens (and have such a transaction be reflected in a distributed ledger) that represent an interest in the securities, rather than the securities themselves.

Of course, tokenization in this manner faces a number of regulatory hurdles – some inherent to the concept itself, and some particular to each specific implementation. For example, as a general matter, it is of particular import that parties do not run afoul of the broad reach of the U.S. securities laws.[3] A particular challenge is the essential dependence of many securities law analyses on the facts and circumstances of each case, precluding a one-size-fits-all approach to compliance: for example, a Transfer Token may well be considered a "security" based on a certain implementation of the concept, but not on others. Additionally, applying a layer of tokenization to traditional activities or transactions raises the broader question of whether regulation should be "technology neutral," and whether well-established legal and regulatory regimes applicable to traditional assets or transactions must (or should) be adapted to account for the development of new technologies such as DLT and tokenization.

The second section of this chapter will provide a basic overview of DLT and how it can be used to create Transfer Tokens that represent underlying assets. The third section provides an overview of the U.S. securities law regulatory framework as applied to

tokens, and describes a "generic" implementation of a Transfer Token. It also discusses how we believe a hypothetical implementation of such a token should be characterized for the purposes of U.S. securities laws. The fourth section will provide two examples of potential uses of Transfer Tokens, along with an overview of certain legal issues germane to each implementation. The fifth section reviews certain regulatory developments that have begun to shed light on how DLT and similar technologies may fit into existing legal and regulatory frameworks. Finally, the sixth section discusses the regulatory environment surrounding "stablecoins," which bear similar characteristics to Transfer Tokens and have gained increasing popularity in recent years.

Background

While a full overview of DLT is outside the scope of this chapter, DLT (commonly implemented in the form of "blockchain" technology) generally refers to a "decentralized peer-to-peer network that maintains a ledger of transactions that utilizes cryptographic tools to maintain the integrity of transactions and some method of protocol-wide consensus to maintain the integrity of the ledger itself."[4] While early implementations of DLT, such as Bitcoin, were limited in scope and intended primarily to facilitate peer-to-peer transfers of value, other implementations of DLT incorporate the ability for parties to "structure and update data on a ledger through robust computer code, known as smart contracts."[5] This allows "any asset or thing [to] be modeled on a ledger," and "parties to run computer functions to interact with the data structures on the ledger."[6]

One potential application of DLT in this context is the ability to "tokenize" a broad range of traditional assets, which, at least theoretically, can encompass nearly anything. In this way, transfers of the asset "can be tracked automatically on a blockchain platform in the same manner as a cryptocurrency such as Bitcoin is tracked using the same technology."[7] By tokenizing an asset and allowing it to be digitally represented on a blockchain or other form of distributed ledger, the process of recording and transferring ownership of the asset can be significantly streamlined. The question of whether such digital assets are "securities" is a critical one, as the application of the securities laws to the issuance and transfer of digital assets such as the Transfer Tokens could impose onerous, and potentially irrational, requirements on the "issuers" of the Transfer Tokens and hamper the ability of secondary market participants to trade Transfer Tokens amongst each other.

Characterization of tokens under securities laws

Background of treatment of digital assets

Beginning in 2017, the Securities and Exchange Commission (the "SEC") has, through various avenues, articulated its general stance toward the regulatory classification and treatment of digital assets. In April 2019, the SEC issued its *Framework for "Investment Contract" Analysis of Digital Assets* (the "SEC Framework"). As described in the SEC Framework, any person "engaging in the offer, sale, or distribution of a digital asset" must "consider whether the U.S. federal securities laws apply," and a threshold issue is "whether the digital asset is a 'security' under those laws."[8] While the framework is new, its essential underpinning is not: central to the SEC's analysis has been, and continues to be, the well-worn, three-prong test articulated by the Supreme Court in *SEC v. W.J. Howey Co.*, 328 U.S. 293 (1946) ("*Howey*"). The *Howey* test "applies to any contract, scheme, or transaction, regardless of whether it has any of the characteristics of typical securities," and is meant to determine whether a particular asset or arrangement is an "investment contract" (and

therefore a security). Under the test established in *Howey*, an "investment contract" exists if there is (i) an investment of money, (ii) in a common enterprise, (iii) with a reasonable expectation of profits derived predominantly from the efforts of others.

In analyzing whether something is a security, "form should be disregarded for substance."[9] The SEC has primarily applied the *Howey* test to digital assets because such assets do not otherwise fall into any of the enumerated categories of the definition of "security." Accordingly, the *Howey* test focuses not only on the form and terms of the asset or arrangement itself, "but also on the circumstances surrounding the digital asset and the manner in which it is offered, sold, or resold (which includes secondary market sales)."[10] As a result, the question of whether a hypothetical Transfer Token is a "security" is one that resists blanket classification, and that instead depends on both the form and function of the Transfer Token as well as the particular facts and circumstances surrounding the issuance, offering, and secondary market transfers of the Transfer Token.

While "[no] one factor is necessarily dispositive as to whether or not an investment contract exists,"[11] the SEC Framework articulates a wide range of factors that would be indicative of the presence of an "investment contract," mapping these factors to each prong of the *Howey* test. These factors include, among others:

- An investment of money: Investors purchase or otherwise acquire the digital asset in exchange for value, whether that value takes the form of fiat currency, another digital asset, or another type of consideration.
- A common enterprise: While the SEC Framework notes that the SEC does not view the "common enterprise" requirement as a distinct element of the *Howey* test, the SEC noted that investments in digital assets have generally constituted investments in a common enterprise "because the fortunes of digital asset purchasers have been linked to each other or to the success of the promoter's efforts."[12]
- Reasonable expectation of profits derived from efforts of others: An investor has a reasonable expectation of profits derived from the efforts of others if a promoter, sponsor, or other third party (each, an "Active Participant" or "AP") provides essential managerial efforts that affect the success of the enterprise, and investors reasonably expect to derive profit from those efforts. While no one factor is determinative, the SEC Framework lists the following factors as indicative of whether this prong is met:
    - the purchaser reasonably expects to rely on the efforts of an AP;
    - the managerial efforts are significant and affect the failure or success of the enterprise, as opposed to efforts that are ministerial in nature;
    - an AP is responsible for the development, improvement, operation, or promotion of the network;
    - where the network or digital asset is still in development or not yet fully functional, investors would reasonably expect an AP to further develop the functionality of the network and/or digital asset;
    - there are essential tasks or responsibilities performed and expected to be performed by an AP;
    - an AP creates or supports a market for, or the price of, the digital asset;
    - an AP has a lead or central role in the direction of the ongoing development or management of the network or the digital asset;
    - investors would reasonably expect the AP to undertake efforts to promote its own interests and enhance the value of the network or digital asset, such as where the AP has the ability to realize capital appreciation from the value of the digital asset, the AP distributes the digital asset as compensation to management, or the AP monetizes the value of the digital asset;

- the digital asset gives the holder rights to share in the enterprise's income or profits or to realize gain from capital appreciation of the digital asset;
- the digital asset is transferable or traded on a secondary market or platform;
- purchasers reasonably would expect the AP's efforts to result in capital appreciation of the digital asset;
- the digital asset is offered broadly to potential purchasers or in quantities indicative of investment intent;
- the AP is able to benefit from its efforts as a result of holding the same class of digital assets as those being distributed to the public;
- the potential profitability of the operations of the network or the potential appreciation in the value of the digital asset is emphasized in marketing or other promotional materials; and
- the availability of a market for the trading of the digital asset.

In contrast, the SEC Framework highlights a number of factors that, while not necessarily determinative, would support the notion that the *Howey* test is not met,[13] including:

- the distributed ledger network and digital asset are fully developed and operational;
- holders of the digital asset are immediately able to use it for its intended functionality on the network;
- the digital asset's creation and structure is designed and implemented to meet the needs of its users, rather than to feed speculation as to its value or development of its network;
- prospects for appreciation in the value of the digital asset are limited;
- any economic benefit that may be derived from appreciation in the value of the digital asset is incidental to obtaining the right to use it for its intended functionality;
- the digital asset is marketed in a manner that emphasizes its functionality rather than the potential for the increase in market value of the digital asset;
- potential purchasers have the ability to use the network and the digital asset for its intended functionality;
- restrictions on the transferability of the digital asset are consistent with the asset's use and not facilitating a speculative market; and
- if the AP facilitates the creation of a secondary market, transfers of the digital asset may only be made by and among users of the platform.

Application of the securities laws and the SEC Framework to Transfer Tokens

As noted above, the question of whether the Transfer Token is a "security" depends on both the form and function of the Transfer Token as well as the particular facts and circumstances surrounding the issuance, offering, and secondary market transfers of the Transfer Token. Provided the aim is to design a Transfer Token such that (i) the hallmarks of a "security" described in the SEC Framework are generally not present, in either form or substance, and (ii) the factors that would indicate that a digital asset is *not* a security *are* present, we imagine a generic Transfer Token with a number of essential characteristics that we believe should, when analyzed through the prism of the factors articulated by the SEC above, cause that Transfer Token to fall outside the definition of security. These characteristics include:

- The Transfer Tokens are issued to represent a specific underlying asset, and are designed for the express purpose of facilitating a transfer of that asset. *Discussion*: In general, the more narrowly tailored the design of the Transfer Token, the less likely it would be to fall under the auspices of the securities laws. For example, in a hypothetical implementation, a holder of a Transfer Token (a "Token Holder") may deposit assets, such as cash or securities, with a custodian, and receive Transfer Tokens representing said cash or securities in return.[14] The Transfer Tokens could then be used to facilitate

transfers of the underlying cash or securities to other market participants who maintain accounts at that custodian. Recipients of Transfer Tokens could, in turn, "redeem" the Transfer Tokens with the custodian in order to receive the underlying cash or securities. Under this model, the Transfer Tokens' creation and use – tied solely to facilitating a transfer of the underlying assets – would more likely be considered to have been designed and structured to meet the needs of users, rather than to feed speculation.

- Note that, given the SEC's broad interpretation of an "investment" of money under the *Howey* test, such an acquirer of Transfer Tokens may nevertheless be considered to be making an "investment" of value. However, the acquirer is not obtaining the Transfer Tokens for investment *purposes*; rather, the acquirer is *exchanging* some form of property for a Transfer Token that represents that property, and subsequently using the resulting Transfer Token to effect a transfer of that property to another party. Crucially, the Transfer Token itself is not purchased because of its value; rather, the Transfer Token should be envisioned as having no value in and of itself, and more akin to a book-entry representing some underlying asset rather than an asset itself.[15]
- Because Transfer Tokens are created to represent specific underlying assets and have no value distinct from those assets, there is no "common enterprise" linking the fortunes of the entity issuing Transfer Tokens to Token Holders, or the fortunes of Token Holders to each other. *Discussion*: While the SEC "does [not] view a 'common enterprise' as a distinct element of the term 'investment contract,'" the SEC Framework notes that "investments in digital assets have constituted investments in a common enterprise because the fortunes of digital asset purchasers have been linked to each other or to the success of the promoter's efforts." In particular, the SEC Framework notes that investors in a digital asset that is a security would reasonably expect capital appreciation in the value of the digital asset based on the efforts of an AP. This is not the case with respect to the Transfer Tokens; Token Holders' fortunes are neither linked to the fortune of the "issuer" of the token nor to the fortunes of other Token Holders. Rather, Token Holders' fortunes are tied only to the value of the underlying asset represented by the Transfer Token, whose value should not be affected by the tokenization of the asset.
- Additionally, because Transfer Tokens are tied to specific underlying assets and designed to facilitate a transfer of those assets, market participants would not acquire the *tokens themselves* with a reasonable expectation of profits predominantly from the efforts of others. *Discussion*: In contrast to scenarios described in the SEC Framework, there is no AP in the transactions imagined in this chapter that would retain the digital asset, or that would support the price of the digital asset, undertake efforts to enhance the value of the digital asset, or have the ability to realize capital appreciation from the value of the digital asset. The Transfer Tokens are created merely to streamline the process by which market participants may transact in certain types of assets and transfer interests among each other. Participants acquire Transfer Tokens not to profit from the efforts of others, but to more easily effectuate the envisaged transaction(s) in the underlying asset.
- The Transfer Tokens imagined would be issued on a functioning network, be designed to replicate and streamline the process normally associated with transacting in the asset represented, and be distributed only among people or institutions that comprise the existing market for the underlying asset. *Discussion*: As noted above, the *Howey* test is less likely to be met if a digital asset's creation and structure is designed and implemented to meet the needs of its users *and* the restrictions on the transferability of the digital asset are consistent with the asset's use. This would generally mean, for

example, that to the extent that purchasers of an underlying asset would be limited to individuals or institutions that meet certain criteria, the issuance and transfer of Transfer Tokens should also be so limited.

- Because the Transfer Tokens are meant to replicate "traditional" interests in the underlying assets represented by the Transfer Tokens, one of the primary policy purposes of the securities laws articulated by the SEC – *i.e.*, compelling disclosure in order to reduce informational asymmetries between promoters and investors – would be inapplicable to the use of Transfer Tokens imagined by this chapter, because no informational asymmetry is produced by the tokenization of an asset. No part of the "traditional" transaction in the asset is in substance altered by tokenization, and as noted above, the creation of Transfer Tokens can be more properly envisioned as the creation of an electronic book-entry representing an underlying asset, rather than the creation of a new asset itself.

Potential applications of Transfer Tokens

Within the model articulated in the foregoing section, Transfer Tokens may be used to streamline transactions in a potentially wide range of assets, although different legal considerations may apply to each. This section reviews the potential applicability of Transfer Tokens to two distinct markets, the syndicated loan market and the market for artwork, and briefly discusses certain relevant considerations with respect to each.

Syndicated loans

Syndicated term loans are traded by a range of sophisticated financial institutions, including commercial banks, investment banks, hedge funds, broker-dealers, and other institutions. One potential application of DLT using Transfer Tokens involves "tokenizing" an interest in a syndicated loan that has been purchased by a lender or secondary market participant pursuant to an assignment or participation. In this way, "[t]he loans held by lenders in a syndicate can be tracked automatically on a blockchain platform in the same manner as a cryptocurrency such as Bitcoin is tracked using the same technology."[16] By tokenizing an asset and allowing it to be digitally represented on a blockchain or other form of distributed ledger, the process of recording and transferring ownership of the asset should be significantly streamlined.

The syndicated loan market is perhaps an ideal candidate for the application of DLT: loans are currently originated (and trades conducted) pursuant to a complicated suite of documentation, which can theoretically be simplified and made more transparent by reflecting the essential terms of such documentation on a blockchain. Additionally, the underlying assets – loan interests – are generally not considered securities, and so the trading of loan interests among financial institutions has not been considered subject to the securities laws.[17] The tokenization of loan interests, then, should not be considered to jeopardize that characterization, *provided* that the tokenization is designed solely to facilitate efficient transfer and record-keeping with respect to secondary market transactions in the interests.

For example, a Transfer Token should be designed such that a Token Holder would own an assignment or participation interest in a syndicated term loan in the same manner as the holder of a "traditional" assignment or participation interest, and the rights and obligations of that Token Holder would likewise be identical to that of a lender purchasing a traditional assignment or participation interest. Furthermore, such Transfer Tokens should be subject to certain restrictions on transfer, such that they could be traded

only among the same sophisticated financial institutions that currently participate in the secondary market for loans, and transfer should be subject to the same restrictions (*e.g.*, the consent of the borrower) that currently apply to the sale and transfer of loan interests. Lastly, we would expect that the Tokens would be issued by the originating financial institutions (or affiliates thereof), transferred through a fully functioning private or public blockchain (which may be developed, operated, and/or maintained by the financial institutions originating or participating in the loan), and would not be made freely available to the public on a secondary market trading platform in a manner inconsistent with the current marketing and sale process applicable to syndicated loans. Such a design should, consistent with the objectives discussed above, minimize the hallmarks of a "security" described in the SEC Framework.

Notwithstanding the foregoing, the *Howey* test *may* be met if the Tokens possessed additional characteristics inconsistent with traditional limitations on the marketing and sale of loan interests. For example, if the Tokens were to be freely tradeable on a secondary market platform among the public or participants who did not have the ability to request information from, or conduct due diligence on, the borrower, such transferability would implicate certain of the important policy considerations of the securities laws and may cause the Tokens to be considered securities. As always, the facts and circumstances are crucial.

Artwork

One perhaps novel use of Transfer Tokens envisioned under this framework would be for transfer of artwork. Transacting in certain types of property under U.S. law can be a complicated exercise, and artwork falls into a category of property that faces certain practical obstacles to transfer. Contemporary art transfers typically involve a trusted intermediary (such as an art dealer or gallery) who agrees to store and present the artwork to potential buyers for a hefty fee.[18] At the same time, these traditional intermediaries offer a necessary legitimizing function, whether it is in reviewing art pieces for authenticity, evaluating the quality of art presented and sold, or collecting artwork under a centralized clearinghouse, which makes it easier for art buyers and sellers to find the pieces they want. As a result, traditional intermediaries create markets for art transactions that otherwise would not exist.

DLT could be used to create more efficient artwork markets. For example, a company dedicated to compiling registries for unique assets recently partnered with a start-up company to auction digital and physical artworks associated with what could be characterized as Transfer Tokens on the Ethereum blockchain platform, with each Transfer Token associated with a unique piece of art.[19] Based on the early success of DLT-facilitated artwork transfers, traditional art houses and galleries have reportedly started experimenting with auctions using blockchain technology to move artwork between interested parties.[20] The benefits of publicly verifiable and secure digital transactions in the art space can be echoed across industries, and the success of DLT as applied to artwork might trigger other innovative uses of Transfer Tokens for other difficult-to-transfer goods.[21]

Regulatory developments

The use of Transfer Tokens, and the advent of new financial technologies more broadly, raises the fundamental question of how assets, activities or transactions that are subject to well-established legal and regulatory regimes should be treated when superimposed with the overlay of new technology. On the one hand, institutions that employ solutions such as DLT in an effort to streamline existing activities or processes, or that propose to conduct traditional activities (such as providing bank custody services) but with respect to assets

such as digital tokens, could be viewed as engaging in the same activities that have always been permissible to them. On the other hand, the use of novel technology could potentially introduce new risks to existing activities, or even alter the essential nature of the underlying activity in ways that warrant additional scrutiny.

While there is unlikely to be a universal answer to this question, recent years have provided some indication of how regulators are beginning to grapple with these issues. Perhaps the issue that has received the most attention is the question of whether digital assets should be considered "securities" subject to the securities laws, as discussed under "Characterization of tokens under securities laws" above. In this area, the SEC has made clear that substance, as analyzed against longstanding precedent, should prevail over form. While the SEC Framework dates to 2019, it fundamentally represents an attempt by the SEC to apply the well-trodden principles set forth in *Howey*, a court case decided in 1946, to the particular qualities germane to digital assets.

While many of the SEC's most visible activities in the digital asset realm have taken the form of enforcement actions against entities conducting unregistered securities offerings, the agency has also shown a willingness to encourage DLT-based market innovation. In testimony before the U.S. Senate in 2019, SEC Chairman Jay Clayton stated that he was "optimistic that developments in distributed ledger technology can help facilitate capital formation, providing promising investment opportunities for both institutional and Main Street investors," adding that he believed the SEC has taken a "measured, yet proactive regulatory approach that both fosters innovation and capital formation while protecting our investors and our markets."[22] In October of 2019, the SEC issued a no-action letter to Paxos Trust Company, LLC ("Paxos") allowing Paxos to conduct a time-limited "feasibility study" involving the use of DLT to facilitate the clearance and settlement of listed U.S. equity securities trades in a production environment involving several large broker-dealers.[23] While a full review of the settlement service offered by Paxos is outside the scope of this chapter, the system bears a number of similarities to the Transfer Tokens described herein: participants in the Paxos system may deposit eligible cash or securities into a settlement account and receive digitized security entitlements in return, which may be used to facilitate the settlement of transactions involving the purchase or sale of such deposited securities. While the SEC's no-action letter to Paxos is strictly limited to the SEC's enforcement stance and declines to address the substance of Paxos' legal conclusions, the letter is a potential indication that the SEC may be receptive to the viability of Transfer Tokens and their use to facilitate securities settlement.[24]

Stablecoins

In the past two years, "stablecoins" ("Stablecoins") have become a subject of significant and increasing regulatory scrutiny. Although they are not technically Transfer Tokens, Stablecoins share with them many overlapping characteristics and regulatory concerns. Stablecoins, a form of cryptocurrency, attempt to tie their value to that of an external reference point, thereby achieving price stability and predictability. The primary mechanism by which Stablecoins peg their value to an underlying asset is collateralization, wherein Stablecoin issuers maintain a reserve of valuable assets (*e.g.*, fiat currencies, commodities, debt, other cryptocurrencies, or a combination thereof) made exchangeable with Stablecoins by contract. USDC, for example, is a coin issued by regulated financial institutions and exchangeable through those institutions for U.S. dollars at a 1:1 ratio. Stablecoins can also

use consensus protocols or algorithms to issue or destroy coin supply (similar to a central bank controlling the supply of circulating currency), or can act on instructions from an "oracle" to respond to external events.

A series of interpretative letters from the Office of the Comptroller of the Currency (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.[25] 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."[26] 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."[27]
- 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.[28] As was the case under the previous interpretive letter, the OCC found that providing such services constituted core banking activities that national banks are free to engage in, subject to effective risk management and compliance with applicable law.[29]
- 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 other permissible payment activities."[30]

All three interpretive letters echoed sentiments expressed by the OCC in an Advance Notice of Proposed Rulemaking (the "ANPR") issued in June 2020, in which the OCC stated that it has "long understood that the banking business is not frozen in time and agrees with the statement made over forty years ago by the U.S. Court of Appeals for the Ninth Circuit: 'the powers of national banks must be construed so as to permit the use of new ways of conducting the very old business of banking.'"[31] At the same time, the ANPR acknowledged that technological changes presented both opportunities and "new challenges and risks," and asked for comment regarding whether certain aspects of the existing bank regulatory framework should be revised to reflect technological advances and innovations.

Taken together with the SEC's recent statements, the OCC pronouncements reinforce the notion that regulators may be willing to embrace technological innovation so long as it is conducted in a sound, responsible manner with an eye toward mitigating any attendant risks. The potential risks, however, could be significant. The OCC guidance cautioned that banks should maintain at least a 1:1 capital reserve ratio for issued Stablecoins,[32] and to "adapt and expand existing [Bank Secrecy Act (the "BSA") and anti-money laundering ("AML")] compliance programs to assure compliance with the reporting and recordkeeping requirements of the BSA and to address the particular risks of cryptocurrency transactions."[33]

The OCC guidance provides some degree of comfort to national banks seeking to issue and provide services related to Stablecoin products. Indeed, they may lead to the shift of Stablecoin management from non-bank players to banks, which already have an established legal framework in which to operate (in addition to the requisite capital requirements, customer base, and compliance programs). As evidence of this trend, several new charter or conversion applications for fintech start-ups have been filed since July 2020.[34] Developments in this area remain ongoing, however, and recent changes in regulatory agency leadership may give pause to bank players seeking to take advantage of what had seemed an increasingly accommodating regime. For example, Michael Hsu, acting Comptroller of the Currency, has recently suggested that the OCC will revisit previous actions in an effort to develop a more coherent federal approach to cryptocurrency regulation, stating that "everything's on the table" in terms of revision of previous agency actions.[35]

Conclusion

Transfer Tokens offer a wide range of possibilities when it comes to streamlining transactions in traditional assets. As reviewed herein, there are strong arguments that the model Transfer Tokens described in this chapter are not securities (or even, in themselves, assets), and that tokenizing an asset to facilitate its transfer should not change the legal or economic substance of the transaction. While the potential applicability of Transfer Tokens is vast, however, market participants must carefully review each implementation – especially when evolving, highly regulated financial markets are involved – to ensure that the attendant legal issues are properly addressed.

* * *

Endnotes

1. It should be noted that the use of the term "digital assets" is somewhat of a misnomer, as assets are typically understood as things that have value. Ideally, the Transfer Token should be conceptualized as akin to a book-entry that has no value in and of itself, but merely represents an underlying asset. Even the use of the word "token" is problematic, as it can both imply value and carry negative connotations associated with the raft of tokens issued pursuant to "initial coin offerings" in recent years. Here, we use the word token to mean that it is *symbolic.*
2. One archetypal example of this concept drawn from traditional markets, of course, is the framework that has developed around the indirect ownership of securities under the Uniform Commercial Code (the "UCC"). In response to a "paperwork crisis" on Wall Street during the 1960s and 1970s, when the burden of reconciling trades using the traditional certificate-based system overwhelmed brokerage firms and transfer agents, the Depository Trust Company ("DTC") was created to act as a central securities depository and hold immobilized share certificates on behalf of its participants. The regulatory scheme that governs transfers of interests in the securities held by DTC is Article 8 of the UCC, which provides that persons holding securities through brokers or custodians hold "security entitlements," rather than direct ownership of the underlying securities. Article 8 describes the package of rights held by the holder of a security entitlement (the "entitlement holder"), and provides that an entitlement holder may issue an "entitlement order" in respect of a financial asset that directs an intermediary to transfer or redeem the financial asset to which the entitlement holder has a security entitlement.

3. The use of "securities laws" in this chapter generally refers to the Securities Act of 1933 together with the Securities Exchange Act of 1934 and the regulations and interpretations issued thereunder.
4. *See* Blockchain and Distributed Ledger Technology: An Analysis of its Impact on the Syndicated Loan Market, Part One: Generation Considerations and Blockchain Primer, LSTA (2018).
5. *Id*.
6. *Id*.
7. *See* Blockchain and Distributed Ledger Technology: An Analysis of its Impact on the Syndicated Loan Market, Part Three: Application of Blockchain Technology to the Loan Market, LSTA (2018).
8. SEC Framework, Section I.
9. *Tcherepnin v. Knight*, 389 U.S. 332, 336 (1967).
10. *Id*.
11. SEC Framework, footnote 4.
12. SEC Framework, footnote 11.
13. The SEC issued, concurrently with the SEC Framework, a no-action letter addressed to an air charter service company proposing to issue "blockchain-based digital assets in the form of 'tokenized' jet cards." In that letter, the SEC stated that it would not recommend enforcement against the company for issuing tokens without registration under the securities laws, because (i) the company would not use the proceeds from its token sale to develop a platform or network, which would be fully developed and operational by the time any tokens were sold, (ii) the tokens would be immediately usable for their intended functionality (*i.e.*, purchasing air charter services) at the time of the sale, (iii) transfers of the tokens would be restricted to the company's wallets, (iv) tokens would be sold at one USD per token throughout the life of the program, and each token represented an obligation by the company to supply air charter services at a value of one USD per token, (v) the company would only offer to repurchase tokens at a discount to their face value, and (vi) the tokens would be marketed in a manner that would emphasize their functionality, rather than the potential for increase in its market value. *See* https://www.sec.gov/divisions/corpfin/cf-noaction/2019/turnkey-jet-040219-2a1.htm. On July 25, 2019, the SEC issued a second no-action letter to a gaming platform operator that proposed to sell "Quarters" to gamers for use in online video games. In that letter, the SEC noted the presence of factors similar to those cited in its previous letter, including that the platform would be fully operational immediately upon its launch (and before the sale of any Quarters), that Quarters would be immediately usable for their intended purpose and transferable only among other wallets on the platform, that Quarters would be made continuously available at a fixed price, and that Quarters would be sold solely for consumptive use as a means of accessing and interacting with participating games. *See* https://www.sec.gov/corpfin/pocketful-quarters-inc-072519-2a1.
14. A custodian, for these purposes, would be a financial institution licensed or chartered to provide custodial services. However, the token *issuer* may be (but is not necessarily required to be) the custodian itself; for example, we envision that token issuances and redemptions may be handled by a third-party company or by a platform maintained and operated by a consortium of institutions. While we generally do not believe the identity of the token issuer should, in itself, alter the analysis or whether the issued tokens are securities, additional analysis may be required regarding whether the activities of

such a company or platform would cause it to fall within the definition of a "clearing agency" subject to registration with the SEC, and if so, whether an exemption from registration would be available.

15. The model Transfer Tokens described in this chapter are distinguishable from cryptocurrencies that are purchased because of their value and that are not typically representative of any underlying asset. Such cryptocurrencies do often bear the hallmarks of investment vehicles. The proposed Diem (formerly "Libra") cryptocurrency, however, broke with the more traditional formulation of blockchain-based cryptocurrencies when it was first introduced in 2019, because it would be backed by a reserve of low-volatility assets, which the creators called the Diem Reserve. While a full discussion of the Diem is beyond the scope of this chapter, Diem, as envisioned by its creators, could be a new type of cryptocurrency with the potential to bring access to low-cost means of transferring money to those who currently have little or no access to financial services. In order to be successful, the creators of the Diem note that it must be more widely adopted than other cryptocurrencies have been to date, citing volatility as one of the major impediments to adoption. In order to alleviate the volatility often associated with blockchain-based cryptocurrencies, Diem would be backed by assets like bank deposits and short-term government securities. Because of this, the Diem could be errantly described as being representative of the assets that support its value. However, the assets that make up the reserve can be viewed more accurately as a tool to decrease volatility and thereby increase potential adoption. The Diem *itself* is intended to have value, and the underlying assets are intended to provide a stable range to that value.

    Therefore, despite the apparent similarity between a formulation of Diem backed by low-volatility assets and the Transfer Tokens proposed by this chapter that are representative of assets having value, the two concepts differ in a way that is crucial to the analysis of the applicability of securities law: the former is intended to have value in and of itself; and the latter is intended to be merely representative of an underlying valuable asset with no intrinsic value of its own. *See* https://www.diem.com/en-us/white-paper/. Diem's 2019 proposal received significant regulatory and legislative pushback from U.S. and foreign governments, and in 2020, the Diem Association (then called the Libra Association) announced that it would modify its proposal to introduce single-currency stablecoins backed by individual national currencies. *See* https://www.diem.com/en-us/updates/finma-payment-system-license/. In December of 2020, Libra was renamed "Diem," and the associated digital wallet (and Facebook subsidiary) was renamed "Novi," in anticipation of a 2021 launch. *See* https://www.coindesk.com/business/2020/12/01/libra-rebrands-to-diem-in-anticipation-of-2021-launch/. However, as of this writing in September 2021, Diem has yet to be launched.
16. *See* Blockchain and Distributed Ledger Technology: An Analysis of its Impact on the Syndicated Loan Market, Part Three: Application of Blockchain Technology to the Loan Market, LSTA (2018).
17. *See Banco Espanol de Credito v. Security Pac. Nat'l Bank*, 973 F.2d 51 (2d Cir. 1992).
18. *See* "How to Approach Selling Art as a Collector," Artwork Archive (2019), *available at* https://www.artworkarchive.com/blog/how-to-approach-selling-art-as-a-collector.
19. *See* R. O'Dywer, "A Celestial Cyberdimension: Art Tokens and the Artwork as Derivative," *Circa Art Magazine* (accessed Jul. 21, 2019), *available at* https://circaartmagazine.net/a-celestial-cyberdimension-art-tokens-and-the-artwork-as-derivative/.

20. H. Neuendorf, "Christie's Will Become the First Major Auction House to Use Blockchain in a Sale," ArtNet News (2018), *available at* https://news.artnet.com/market/christies-artory-blockchain-pilot-1370788.
21. *See* "Blockchain in Oil & Gas," Deloitte (accessed Jul. 21, 2019), *available at* https://www2.deloitte.com/us/en/pages/consulting/articles/blockchain-digital-oil-and-gas.html.
22. *See* Testimony on "Oversight of the Securities and Exchange Commission" Before the U.S. Senate Committee on Banking, Housing, and Urban Affairs, *available at* https://www.sec.gov/news/testimony/testimony-clayton-2019-12-10 (Dec. 10, 2019).
23. *See* Letter from Jeffrey S. Mooney, Associate Director, SEC, to Charles G. Cascarilla & Daniel M. Burstein, Paxos Trust Company, LLC, *available at* https://www.sec.gov/divisions/marketreg/mr-noaction/2019/paxos-trust-company-102819-17a.pdf (Oct. 28, 2019).
24. On September 25, 2020, the SEC issued a no-action letter permitting registered broker-dealers that meet certain requirements to operate alternative trading systems ("ATS") that trade digital asset securities, provided the ATS is organized such that: (i) a buyer and seller send their respective orders to the ATS, notify their respective custodians of such orders, and instruct their respective custodians to settle transactions in accordance with the terms of their orders when the ATS notifies the custodians of a match on the ATS; (ii) the ATS matches the orders; and (iii) the ATS notifies the buyer and seller of their respective custodians of the matched trade, upon which the custodians would settle the trade on behalf of the buyer and seller. *See* Letter from Elizabeth Baird, Deputy Director, Division of Trading and Markets, SEC, to Kris Dailey, Financial Industry Regulatory Authority, *available at* https://www.sec.gov/divisions/marketreg/mr-noaction/2020/finra-ats-role-in-settlement-of-digital-asset-security-trades-09252020.pdf (Sept. 25, 2020).
25. *See* Interpretive Letter #1170, OCC, *available at* https://www.occ.gov/topics/charters-and-licensing/interpretations-and-actions/2020/int1170.pdf (Jul. 22, 2020).
26. *Id.*
27. *Id*.
28. *See* Interpretive Letter #1172, OCC, *available at* https://www.occ.treas.gov/topics/charters-and-licensing/interpretations-and-actions/2020/int1172.pdf (Sept. 21, 2020). On September 21, 2020, SEC staff issued a statement regarding this OCC 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. The SEC statement is *available at* https://www.sec.gov/news/public-statement/sec-finhub-statement-occ-interpretation.
29. *See* Interpretive Letter #1172, OCC, *available at* https://www.occ.treas.gov/topics/charters-and-licensing/interpretations-and-actions/2020/int1172.pdf (Sept. 21, 2020).
30. *See* Interpretive Letter #1174, OCC, *available at* https://www.occ.treas.gov/topics/charters-and-licensing/interpretations-and-actions/2021/int1174.pdf (Jan. 4, 2021).
31. *See National Bank and Federal Savings Association Digital Activities*, Advance Notice of Proposed Rulemaking, *available at* https://www.occ.gov/news-issuances/news-releases/2020/nr-occ-2020-76a.pdf.
32. *See* Interpretive Letter #1174, OCC, *available at* https://www.occ.treas.gov/topics/charters-and-licensing/interpretations-and-actions/2021/int1174.pdf (Jan. 4, 2021).
33. *Id.*
34. *See*, *e.g.*, Conditional Approval #1205 [Varo Bank, N.A.], OCC, *available at* https://www.occ.gov/topics/charters-and-licensing/interpretations-and-actions/2018/ca1

205.pdf (Aug. 31, 2018); Figure Applies for National Bank Charter From the OCC, Business Wire, *available at* https://www.businesswire.com/news/home/20201106005466/en/Figure-Applies-for-National-Bank-Charter-From-the-OCC (Nov. 6, 2020); Letter from Stephen A. Lybarger, Deputy Comptroller for Licensing, OCC, to Sara Lenet and Tim Bogan, LendingClub Corporation, *available at* https://www.occ.treas.gov/topics/charters-and-licensing/decision-letter-lending-club.pdf (Dec. 30, 2020).

35. *See* OCC's Hsu Says Crypto Charters 'On The Table' In Review, *Law360*, *available at* https://www.law360.com/articles/1390258/occ-s-hsu-says-crypto-charters-on-the-table-in-review (Jun. 2, 2021).

* * *

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.

James Kong
Tel: +1 212 819 8245 / Email: james.kong@whitecase.com

James has significant experience in financial regulatory and compliance matters, particularly with respect to the Volcker Rule, authority and control issues arising under the Bank Holding Company Act, resolution planning, US anti-money laundering laws and regulations, non-bank licensing issues, enhanced prudential standards, margin regulations, and Title VII of the Dodd-Frank Act. He also has particular experience advising on cyber security and financial technology regulatory matters.

James frequently publishes articles regarding timely regulatory developments. He has been invited to speak on various financial regulatory panels, including on the topic of secured lending and digital assets and the regulatory environment in the US, Europe and Asia at the IIB's Banking Seminar on Fintech and Digital Assets.

Ben Elron
Tel: +1 202 729 2968 / Email: ben.elron@whitecase.com

Ben is a litigator in White & Case's Washington, D.C. office, where he represents clients in a variety of civil and criminal White Collar matters and in complex commercial disputes. Ben also advises clients on the legal and regulatory landscape for blockchain and digital asset projects, with a focus on securities guidance and enforcement governing the offering and sale of cryptocurrencies.

Ben clerked with the Department of Justice, where he prosecuted complex cybercrime and criminal fraud cases, and brings further experience as a technology strategist and management consultant.

White & Case LLP

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

Ransomware and cryptocurrency: Part of the solution, not the problem

Katie Dubyak, Jason Weinstein & Alan Cohn
Steptoe & Johnson LLP

As ransomware attacks continue to make global headlines with greater frequency, the media and policymakers have tended to portray the issue as a cryptocurrency problem, when in reality it is a cybercrime and cybersecurity problem. Although cryptocurrencies have become an increasingly common means by which ransom is paid, the reality is that ransomware attacks were a problem since before cryptocurrencies existed, and long before the term "cryptocurrency" became part of our cultural vocabulary. And while cryptocurrencies have changed the way that ransoms are paid, their underlying blockchain technology is also a critically important tool for investigating and prosecuting these attacks.

This chapter provides an overview of the legal and regulatory framework that has developed to address ransomware attacks, assesses the role of cryptocurrency and blockchain technology in these cases, and addresses considerations for preventing these attacks from occurring, as well as best practices for responding to an attack if, or when, one occurs.

Background on ransomware

Ransomware attacks typically involve a hacker using malicious software to encrypt or exfiltrate a company's data or other systems, and then demanding the payment of a ransom for a decryption key that allows the target to unlock its systems. In some instances, the hacker may demand a double ransom – one payment for a decryption key, and a second payment to prevent the hacker from disclosing private information gained during the attack. Increasingly, hackers are demanding these ransom payments in cryptocurrency in the belief that doing so better conceals their identities.

The U.S. Department of Justice (DOJ) and Federal Bureau of Investigation (FBI) have been sounding the alarm about ransomware as a serious and growing form of cybercrime threat, and encouraging at-risk businesses to review their cybersecurity posture, since at least 2011[1] – back when Bitcoins were being used to buy alpaca socks and the occasional pizza, and not much else. That warning was well founded, but too often unheeded. In recent years, ransomware attacks have become more sophisticated in both their tactics and scope. Reports have found that the average ransom payment made in 2020 increased by 171% from the previous year, and that the total amount of ransoms paid in 2020 increased by over 300%.[2] These impacts have been particularly pronounced in the healthcare sector, where 92 ransomware attacks in 2020 alone resulted in over $20 billion in losses stemming from ransoms paid impacted revenue, and lawsuits.[3]

The business model for ransomware attacks has also evolved over time to permit less technologically sophisticated actors from perpetrating these attacks. Many ransomware developers now offer a ransomware-as-a-service (RaaS) arrangement, wherein a developer of malicious software licenses the software to affiliates, who in turn identify victims,

carry out the attacks, and coordinate the logistics of ransom payments. As ransomware attacks become an increasingly profitable form of cybercrime, an entire ecosystem of services has developed to support them – including hosts who refuse to cooperate with law enforcement, "crypters" who help perpetrators ensure that their malware will not be identified by antivirus software, and "mixers" and "tumblers" who help launder the illicit cryptocurrency ransom payments.

Ransomware attacks have also become significantly more prevalent in the last few years as the COVID-19 pandemic has caused increased reliance on the cyber world to conduct business. The FBI has reported that the number of complaints rose from 1,493 complaints (with $3.62 million in losses) in 2018 to 2,474 complaints (with losses of over $29.01 million) in 2020.[4]

Indeed, in 2021 there were several notable ransomware attacks that made global headlines. In April 2021, hackers were able to significantly disrupt gas supplies along the entire east coast of the United States through an attack on Colonial Pipeline Company. Although U.S. authorities were able to recover most of the $4.4 million Bitcoin payment that the company was forced to pay, they have still not found the hackers responsible for the attack. Only a month later, in May 2021, the D.C. Metropolitan Police Department was the target of an attack by Russian hacker group Babak. The Police Department's refusal to pay the demanded ransom of $4 million resulted in the release of hundreds of police officer disciplinary files, intelligence reports, and other confidential information. And in June 2021, a hack on U.S. meat supplier JBS USA Holdings Inc. temporarily shut down one-fifth of the United States' beef production capacity, resulting in the payment of $11 million in Bitcoin to the Russian hacker group REvil.

As these recent attacks highlight, ransomware attacks can severely impact a company's ability to do business, and wreak havoc on the industries in which the target companies operate. They also have the potential to impact national security and critical infrastructure, as the Colonial Pipeline attack made clear. In instances where a double ransom is demanded, these attacks can also implicate data privacy and data breach notification laws, and leave companies vulnerable to related litigation. Finally, where the ransom is paid to a sanctioned individual or into a sanctioned jurisdiction, agreeing to pay a ransom can expose the target – and any third-party service processors they use – to the risk of violating U.S. sanctions or other anti-money laundering (AML) laws.

Oversight and regulatory guidance on ransomware attacks

OFAC and FinCEN

On October 1, 2020, the U.S. Department of the Treasury's Office of Foreign Assets Control (OFAC) and Financial Crimes Enforcement Network (FinCEN) published advisories on the sanctions and AML risks associated with facilitating ransomware payments.[5]

The OFAC Advisory explains that OFAC has designated numerous malicious ransomware cyber actors and those who facilitate ransomware transactions under its cyber-related sanctions programme as Specially Designated Nationals and Blocked Persons (SDNs), and that U.S. persons are generally prohibited from dealing with SDNs. Additionally, although the perpetrators of ransomware attacks may not be on OFAC's SDN List, it is possible that they are located within a jurisdiction subject to a U.S. sanctions regime – currently, Iran, North Korea, Syria, Cuba, and the Crimea region of Ukraine – or could be affiliated with the governments of those jurisdictions, including any departments, branches, state-owned enterprises, officers, or agents thereof.

The OFAC Advisory states that making or facilitating a ransomware payment to an attacker on the SDN List or located within a sanctioned jurisdiction may violate U.S. sanctions laws. Additionally, the Advisory notes that "[c]ompanies 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, not only encourage future ransomware payment demands but also may risk violating OFAC regulations". Further, the Advisory notes that OFAC may impose civil penalties for sanctions violations based on strict liability – meaning that a person or entity may be held civilly liable even if it did not know or have reason to know that it was engaging in a prohibited transaction.

The OFAC Advisory encourages financial institutions and other companies involved in potentially facilitating ransomware payments to implement a risk-based compliance programme to mitigate exposure to possible sanctions-related violations. It also advises victims to report ransomware attacks if they believe a ransomware payment may involve a sanctions nexus, and notes that OFAC will "consider a company's self-initiated, timely, and complete report of a ransomware attack to law enforcement to be a significant mitigating factor in determining an appropriate enforcement outcome if the situation is later determined to have a sanctions nexus".

Likewise, the FinCEN Advisory also admonishes victims and companies that paying ransoms may implicate FinCEN's regulations. According to the FinCEN Advisory, because processing ransomware payments is typically a multi-step process that involves at least one depository institution and one or more money services businesses (MSBs), facilitating these payments may constitute money transmission. This, in turn, could trigger the obligation to register as an MSB with FinCEN, and subject the entity to Bank Secrecy Act obligations, including the filing of suspicious activity reports.

The FinCEN Advisory sets forth a list of what it calls "red flag indicators" to assist financial institutions in detecting, preventing, and reporting suspicious transactions associated with ransomware attacks, but explains that no indicator on its own is indicative of illicit activity. These indicators include, among others: (1) suspicious enterprise IT activity that occurs in financial institution system log files, network traffic, or file information; (2) customer notification that a specific payment is in response to a ransomware incident; (3) a customer's cryptocurrency address appears on open sources that have linked the address to ransomware activity; (4) a major transaction occurs between a large company and a cybersecurity incident response firm or cyber insurance provider; (5) a customer receives funds, and then shortly thereafter sends an equivalent amount to a virtual currency exchange; and (6) a customer who shows limited knowledge of virtual currency during interactions with the financial institution enquires about or purchases virtual currency, particularly in large amounts or with a rush request.

In addition to this October 1, 2020 Advisory, in June 2021 FinCEN released its AML priorities, including cybercrime among its top priorities and describing ransomware attacks as a "particularly acute concern".[6] The guidance notes that ill-gotten gains through cybercrime, including ransomware attacks, are often laundered through various means, including rapid transfers through accounts belonging to the cyber actors or money mules. The guidance observes that "[c]overed institutions are uniquely positioned to observe the suspicious activity that results from cybercrime" and encourages financial institutions to share information on suspicious cyber activity under a safe harbour provision of the Bank Secrecy Act. Finally, the guidance stresses that the U.S. government is committed

to "working with like-minded partners around the world to disrupt and deter ransomware actors, including by developing cohesive and consistent policies towards ransom payments and enabling rapid tracing and interdiction of virtual currency proceeds".

In September 2021, it was reported that the Biden Administration plans to use a wide array of actions, including sanctions, to make it more difficult for hackers to use digital currency to profit from ransomware attacks.[7] Consistent with this admonition, on September 21, 2021, OFAC announced its first-ever set of sanctions against a cryptocurrency exchange for its alleged role in facilitating cryptocurrency transactions for ransomware attackers.[8] Concurrent with this announcement, OFAC released an update to its October 2020 guidance on ransomware attacks to add explicit language that the "U.S. government strongly discourages all private companies and citizens from paying ransoms or extortion demands and recommends focusing on strengthening defensive and resilience measures to prevent and protect against ransomware attacks".[9]

Department of Justice

Shortly after OFAC and FinCEN released their October 2020 guidance on ransomware, DOJ's Cyber-Digital Task Force released an Enforcement Framework for Cryptocurrency, which stresses DOJ's aggressive approach toward illicit activities involving cryptocurrency.[10] With respect to ransomware attacks, the Framework observes that cryptocurrency is being used with increasing frequency to facilitate ransom payments. The report notes that the wire fraud statute, 18 U.S.C. § 1343, and the statute related to fraud and intrusions in connection with computers, 18 U.S.C. § 1030, may be used as tools to prosecute ransomware attackers.

Consistent with DOJ's emphasis on aggressively pursuing abusive cryptocurrency practices, in April 2021, news outlets reported that DOJ had internally announced the creation of a task force to curtail the proliferation of ransomware attacks.[11] The task force's goals include devising ways to increase training and resources to address ransomware attack risks, boosting intelligence gathering, and leveraging investigative leads, including connections between cybercriminal gangs and nation-state groups.

A few months later, in June 2021, DOJ released guidance regarding investigations related to ransomware and digital extortion.[12] The guidance states that recent ransomware attacks, including the attack on Colonial Pipeline, "underscore the growing threat that ransomware and digital extortion pose to the Nation, and the destructive and devastating consequences ransomware attacks can have on critical infrastructure". The guidance observes that in order to combat these attacks, prosecutors must enhance and centralise the internal tracking of investigations and prosecutions of ransomware groups, and coordinate with other key law enforcement agencies.

Specifically, the guidance directs assistant U.S. attorneys (AUSAs) to immediately notify the DOJ Criminal Division's Computer Crime and Intellectual Property Section (CCIPS) and the National Security & Cyber Crime Coordinator for the Executive Office for United States Attorneys of the opening of or any significant developments in a ransomware case. AUSAs must also file an Urgent Report whenever they learn of a new ransomware attack in their districts, and coordinate investigations of these attacks with CCIPS.

Moreover, in July 2021, DOJ and the Department of Homeland Security (DHS) announced a new initiative to combat the threat of ransomware through the creation of a website, StopRansomware.gov, designed to be a centralised hub across all federal agencies for ransomware resources.[13] The website integrates federal ransomware resources into a single platform that includes guidance on how to report attacks, and the latest ransomware-related alerts and threats from all participating agencies.

Securities and Exchange Commission

The Securities and Exchange Commission (SEC) has also raised the alarm regarding the risk of ransomware attacks. In July 2020, the SEC released an alert based on its perceived increase in the sophistication of ransomware attacks on SEC registrants, as well as the impact that these attacks have on service providers to registrants.[14] The alert encourages registrants to monitor cybersecurity alerts published by the DHS Cybersecurity and Infrastructure Security Agency (CISA), and to share this information with their third-party service providers, particularly if they maintain client assets and records.

Additionally, although the alert recognises that there is no "one-size-fits-all" approach that can be used to mitigate the risk of these attacks, the SEC provides a list of measures to consider, including (i) regularly updating a company's incident response and resiliency policies, (ii) assessing the systems and processes that are capable of being restored during a disruption so that business can continue to be delivered, (iii) providing training around cybersecurity risks and best practices, (iv) implementing proactive vulnerability and patch management programmes, (v) managing user access through systems and procedures, such as regular password updates and multi-factor authentication, and (vi) implementing security measures designed to control, monitor, and inspect network traffic to prevent problematic traffic.

Legislative action

In addition to the guidance and analysis that government agencies have provided related to ransomware, Congress has also begun to weigh in on the issue through proposed legislative action. On July 27, 2021, the Senate Judiciary Committee convened a hearing entitled "America Under Cyber Siege: Preventing and Responding to Ransomware Attacks". Estimating that only about a quarter of ransomware intrusions are actually reported, representatives of DOJ, the FBI, the U.S. Secret Service, and CISA encouraged Congress to require companies that have been subject to a cyber-attack to notify federal authorities, in an effort to help the government understand the threat of these attacks. These representatives observed that although there are laws requiring companies to notify consumers if their data is leaked in a double ransom attack, there are currently no disclosure requirements for the payment of a single ransom.

Notably, in his remarks at the hearing, Deputy Assistant Attorney General Richard Downing observed that DOJ has begun to devote a significant amount of resources to identifying and prosecuting ransomware actors, dismantling their technical and financial systems, and seizing the illicit virtual currency obtained from the attacks. Nonetheless, Downing stated that combatting ransomware "requires a whole-of-society response, including coordinated action by agencies across the federal government, collaboration with foreign partners, and assistance from victims and the private sector".[15]

Answering this cry for action – and in part motivated by the devastation caused by the Colonial Pipeline attack earlier in the year – Congress introduced at least five bipartisan bills in the summer of 2021 alone designed to address ransomware attacks. This included:

- The International Cybercrime Prevention Act, introduced on June 17, 2021, which aims to increase criminal penalties for cybercrimes, including ransomware attacks, that target critical infrastructure. This bill would, among other things, allow authorities to confiscate communication devices and other property used to commit cybercrime, enhance prosecutors' ability to shut down botnets and other digital infrastructure used for a wide range of illegal activity, and create a new criminal violation for individuals who have knowingly targeted critical infrastructure, including dams, power plants, hospitals, and election infrastructure.

- The Study on Cyber Response Options Act, introduced on June 30, 2021, which would direct DHS to study the risks and benefits of allowing private organisations to conduct offensive cyber operations, since under current law, only the federal government is permitted to do so.
- The Cyber Incident Notification Act of 2021, introduced on July 21, 2021, which would require companies that operate critical infrastructure, such as emergency services, telecommunication networks, and water utilities, to notify DHS within 24 hours after being subject to a ransomware attack.
- The DHS Industrial Control Systems Capabilities Enhancement Act, introduced on July 22, 2021, which would require CISA to ensure that it can better identify and mitigate threats to industrial control systems, the technology involved in the operation of critical infrastructure networks such as pipelines and water and electric utilities.
- The Sanction and Stop Ransomware Act, introduced on August 5, 2021, which is aimed at strongly discouraging foreign countries from providing safe haven to ransomware perpetrators. The bill would require development of cybersecurity standards for critical infrastructure, tighten regulation of cryptocurrency, and direct the State Department and intelligence community to designate as a "state sponsor of ransomware" any country deemed to provide support for ransomware schemes.

Although some of these bills perpetuate the misconception that cryptocurrency is to blame for the rise in ransomware attacks by focusing on the need to increase the regulation of cryptocurrency, they reflect increased attention on the ransomware problem at all levels of the U.S. government.

The role of cyber insurance in ransomware attacks

The insurance industry sells policies to cover losses in the event of a ransomware attack, including business interruption losses, data restoration costs, incident response costs, and the ransom payment itself. These firms can also provide critical support to victims by connecting them to law enforcement and recovery experts, which in turn increases available information about these attacks. Insurance firms have reported that ransomware attacks are now the most common type of reported cyber-related claim.

Although many insurance providers require their clients to adhere to strong security practices to receive coverage – thus potentially disrupting these attacks from occurring in the first place – some commentators have argued that cyber insurance actually proliferates these attacks because victims are more likely to pay a ransom if they know the cost is covered. Indeed, there is some evidence to corroborate this view, as ransomware perpetrators themselves have acknowledged that they often target companies known to have cyber insurance policies.

Cryptocurrencies as tools for investigating attacks and recovering proceeds

Not only is cryptocurrency not to blame for the problem of ransomware attacks, it can actually be part of the solution. With a public, traceable, immutable, borderless ledger of every transaction ever conducted, cryptocurrencies and blockchain technology allow law enforcement to follow the money in a way that would not be possible with cash or many other forms of payment, and even to recover criminal proceeds. Moreover, these continually improving analytics capabilities enhance law enforcement's capacity to identify malicious actors – to "put fingers at the keyboard".

Indeed, the Colonial Pipeline attack in April 2021 – where DOJ was able to recover over $2 million of the ransom – highlights the investigative opportunities presented by cryptocurrencies, and the potential for law enforcement to use this technology to vigorously investigate and prosecute the perpetrators of these attacks.

Considerations for combatting ransomware attacks

The best way of combatting a ransomware attack is to prevent it from occurring in the first place. And the best way of preventing a ransomware attack is the same as the best way of preventing any other type of cyber-attack. That's because ransomware is, plain and simple, a consequence of a successful cyber intrusion. In other words, ransomware is only possible because a bad actor has completed a successful attack on a company's network, whether through phishing or other means. If the hacker can't get into the company's systems, it can't demand the ransom.

So, what should companies do? Among other measures, companies should update their intrusion prevention systems frequently, conduct regular back-up of systems and ensure that back-ups are protected from potential ransomware attacks, and develop and test incident response plans. Information technology administrators should also take steps to continually strengthen the security posture of their organisation by, among other things, maintaining up-to-date antivirus software and operating system patches, restricting access to file and printer sharing services and software installation capabilities, and enforcing strong password and authorisation policies. Companies should also regularly train their employees to educate them on the tell-tale signs of phishing and other types of cyber-attacks and how to respond when faced with a potential attack.

None of these measures are new, because cybercrime is not new. Dating all the way back to the earliest big hacking cases – from TJX to Sony to Target, and many other cases along the way – DOJ, the FBI, DHS, the U.S. Secret Service, and other agencies have been advising companies for decades to take these and other measures in advance of a possible cyber-attack to mitigate the risk of an attack and the consequences if one occurs. In those early cases, the risk was the theft of vast troves of credit card and other customer identity data; now, it's the payment of a ransom. But the underlying crime is the same, and the measures to prevent it are largely the same.

Even with all of these and other protections in place, ransomware attacks – like other types of cyber-attacks – will happen. In the event of an attack, victims should first collect as much information about the attack as they can, including, if available: (i) the name, address and handle of the attacker; (ii) the method in which the attack occurred (*e.g.*, spoofed email, similar domain, etc.); (iii) the ransomware variant name, type, and software language; (iv) the date of the demand and the time for payment before adverse action is taken; (v) the amount and type of payment demanded; (vi) the blockchain wallet addresses indicated to which payment should be made; and (vii) any blockchain analytics available for the wallets or identifiable mixers involved.

Given OFAC's recent guidance on ransomware attacks, before determining whether to make a payment, a victim should consider whether the perpetrator involves a sanctioned individual or entity, and whether it is possible that the payment could implicate a sanctioned jurisdiction. A victim must also consider whether they have a duty to contact law enforcement, including OFAC, the FBI, DHS, or other agencies. Even without a duty to report, contacting law enforcement may be advisable. U.S. financial institutions that fall victim to an attack need to also consider whether they should submit a suspicious activity report.

Additionally, if a double ransom is demanded, the victim must also consider the data privacy implications of failing to pay the ransom under applicable data protection laws.

In short, a company that is the victim of a ransomware attack is at risk of being victimised all over again, this time by an enforcement action based on the circumstances of the payment or by litigation.

As a result, a company that is the victim of a ransomware attack must balance the business and legal risks of not making the payment with the business and legal risks of making the payment. And it must do so under extraordinary pressure. Hardening a company's systems in advance will reduce its risk of an attack. Developing and testing response plans with the benefit of counsel will reduce the company's risk of being victimised by government agencies or plaintiffs' lawyers based on its response to the attack.

* * *

Endnotes

1. *See*, *e.g.*, U.S. Dept. of Justice Press Release, Department of Justice Takes Action to Disable International Botnet (Apr. 13, 2011), available at https://www.justice.gov/opa/pr/department-justice-takes-action-disable-international-botnet (then Assistant Attorney General Lanny A. Breuer stating "Law enforcement will continue to use innovative and responsible actions in our fight against cyber criminals and at the same time, we urge consumers to ensure they are continually taking prudent measures to guard against harm, including routinely updating anti-virus security protection").
2. Institute for Security and Technology, Combating Ransomware – A Comprehensive Framework for Action: Key Recommendations from the Ransomware Task Force (Apr. 2021), available at https://securityandtechnology.org/wp-content/uploads/2021/04/IST-Ransomware-Task-Force-Report.pdf.
3. Comparitech, Ransomware attacks on US healthcare organizations cost $20.8bn in 2020 (Mar. 10, 2021), available at https://www.comparitech.com/blog/information-security/ransomware-attacks-hospitals-data/.
4. Federal Bureau of Investigation, Internet Crime Complaint Center, 2018 Internet Crime Report, available at https://pdf.ic3.gov/2018_IC3Report.pdf; Federal Bureau of Investigation, Internet Crime Complaint Center, 2020 Internet Crime Report, available at https://www.ic3.gov/Media/PDF/AnnualReport/2020_IC3Report.pdf.
5. U.S. Dept. of the Treasury, Office of Foreign Assets Control, Advisory on Potential Sanctions Risks for Facilitating Ransomware Payments (Oct. 1, 2020), available at https://home.treasury.gov/system/files/126/ofac_ransomware_advisory_10012020_1.pdf; U.S. Dept. of the Treasury, Financial Crimes Enforcement Network, Advisory on Ransomware and the Use of the Financial Systems to Facilitate Ransom Payments (Oct. 1, 2020), available at https://www.fincen.gov/sites/default/files/advisory/2020-10-01/Advisory%20Ransomware%20FINAL%20508.pdf.
6. U.S. Dept. of the Treasury, Financial Crimes Enforcement Network, Anti-Money Laundering and Countering the Financing of Terrorism National Priorities (June 30, 2021), available at https://www.fincen.gov/sites/default/files/shared/AML_CFT%20Priorities%20(June%2030%2C%202021).pdf.
7. *Wall Street Journal*, U.S. to Target Crypto Ransomware Payments With Sanctions (Sept. 17, 2021), at https://www.wsj.com/articles/u-s-to-target-crypto-ransomware-payments-with-sanctions-11631885336?mod=politics_lead_pos1.

8. U.S. Dept. of the Treasury, Publication of Updated Ransomware Advisory; Cyber-related Designation (Sept. 21, 2021), available at https://home.treasury.gov/policy-issues/financial-sanctions/recent-actions/20210921.
9. U.S. Dept. of the Treasury, Office of Foreign Assets Control, Updated Advisory on Potential Sanctions Risks for Facilitating Ransomware Payments (Sept. 21, 2021), available at https://home.treasury.gov/system/files/126/ofac_ransomware_advisory.pdf.
10. U.S. Dept. of Justice, Report of the Attorney General's Cyber-Digital Task Force: Cryptocurrency Enforcement Network (Oct. 8, 2020), available at https://www.justice.gov/ag/page/file/1326061/download.
11. CNN, Justice Department is launching a ransomware task force (Apr. 21, 2021), available at https://www.cnn.com/2021/04/21/tech/ransomware-doj-task-force/index.html.
12. U.S. Dept. of Justice, Office of the Deputy Attorney General, Memorandum for All Federal Prosecutors, Guidance Regarding Investigations and Cases Related to Ransomware and Digital Extortion (June 3, 2021), available at https://www.justice.gov/dag/page/file/1401231/download.
13. U.S. Dept. of Justice Press Release, U.S. Government Launches First One-Stop Ransomware Resource at StopRansomware.gov (July 15, 2021), available at https://www.justice.gov/opa/pr/us-government-launches-first-one-stop-ransomware-resource-stopransomwaregov.
14. Securities and Exchange Commission, Office of Compliance Inspections and Examinations, Cybersecurity: Ransomware Alert (July 10, 2020), available at https://www.sec.gov/files/Risk%20Alert%20-%20Ransomware.pdf.
15. Statement of Richard W. Downing before the Committee on the Judiciary of the United States Senate (July 27, 2021), available at https://www.judiciary.senate.gov/download/richard-downing-727-testimony.

Katie Dubyak
Tel: +1 202 429 6413 / Email: kdubyak@steptoe.com

Katie Dubyak, an Associate at Steptoe & Johnson LLP, concentrates her practice on white-collar criminal defence, internal investigations, and other regulatory inquiries. Her clients include both individuals and companies, and span various sectors including blockchain and cryptocurrency, finance, technology, and life sciences. Katie has broad experience in fact development and witness interviews, motion practice, trials, and complex document management issues. She has defended clients against a wide range of allegations, including mail and wire fraud, conspiracy, obstruction, FCPA, money laundering, export controls, and sanctions violations.

Jason Weinstein
Tel: +1 202 429 8061 / Email: jweinstein@steptoe.com

Jason Weinstein is Partner at Steptoe & Johnson LLP, co-chair of the firm's Blockchain and Cryptocurrency practice, and Director to the Blockchain Alliance. He has represented just about every type of participant in the blockchain ecosystem and is widely recognised as one of the leading defence attorneys in government enforcement matters relating to cryptocurrencies. Jason previously served as deputy assistant attorney general in the Department of Justice's Criminal Division, where he supervised the computer crime and organised crime sections, and oversaw numerous investigations involving the use of digital currencies. Jason serves on the advisory boards of Coin Center and the Chamber of Digital Commerce. He also serves as an advisor to Bitfury, the leading full-service blockchain technology company and one of the largest private infrastructure providers in the industry.

Alan Cohn
Tel: +1 202 429 6283 / Email: acohn@steptoe.com

Alan Cohn is Partner at Steptoe & Johnson LLP, co-chair of the firm's Blockchain and Cryptocurrency practice, and Counsel to the Blockchain Alliance. Alan counsels companies on cybersecurity, blockchain and distributed ledger technology, and national security issues. Alan is ranked among the top U.S. lawyers in Blockchain and Cryptocurrencies by *Chambers USA* (2019–2021), where he is noted for his "tremendous depth of expertise in regulatory issues facing blockchain platforms and cryptocurrencies". He previously served in senior policy and management positions at the U.S. Department of Homeland Security for almost a decade, most recently as the Assistant Secretary for Strategy, Planning, Analysis & Risk and second-in-charge overall of the DHS Office of Policy. Alan also serves as an advisor to several technology companies.

Steptoe & Johnson LLP

1330 Connecticut Avenue, NW, Washington, D.C. 20036, USA
Tel: +1 202 429 3000 / URL: www.steptoe.com

A day late and a digital dollar short: Central bank digital currencies

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

"You can count on the Americans to do the right thing after exhausting the alternatives."[1] As China, the fastest growing economy in the world, actively works to its central bank digital currency ("CBDC"), the United States has not launched a pilot digital currency or issued a formal position paper on the creation of a digital currency. It appears the slow and steady approach is being set by Jerome Powell, the Chairman of the Federal Reserve, who has noted that with respect to the creation of a U.S. CBDC, "[i]t is far more important to get it right than it is to do it *fast*".[2]

The creation of a digital currency is being discussed by U.S. lawmakers, the Secretary of the Treasury, and Federal Reserve staff. Senator Elizabeth Warren noted during a recent hearing:

> *Central bank digital currency ... has great promise*. Legitimate digital public money could help drive out bogus digital private money, while improving financial inclusion, efficiency, and the safety of our financial system—if that digital public money is well-designed and efficiently executed ...[3]

One apparent supporter of blockchain technology is former Chairman of the Federal Reserve Bank and current Treasury Secretary Janet Yellen, who has noted:

> *It makes sense for central banks to be looking at [central bank digital currencies] ...* We do have a problem with financial inclusion. Too many Americans really don't have access to easy payment systems and to banking accounts, and I think this is something that a digital dollar – a central bank digital currency – could help with. I think it could result in faster, safer and cheaper payments.[4]

The United States appears to be *exploring* the creation of a digital currency while other countries and the International Monetary Fund ("IMF") have embraced the fact that "CBDC[s] could be the next milestone in the evolution of money".[5] Some experts believe the United States is unaware that it is in a race with China and other nations to develop a CBDC and that the United States could be "*at least a decade away* from using a [CBDC] backed by the [Federal Reserve]".[6] The question is whether the United States will be, or *already is*, a day late and a dollar short in the creation of a digital dollar.

This chapter introduces readers to: (i) the foundations of the operation of traditional currencies and payment systems; (ii) blockchain (distributed ledger) technology, which underpins digital currencies; several of the CBDCs that are currently in development by Sweden, Canada, and China; (iii) some of the issues the United States must address to launch a CBDC; and (iv) the potential privacy concerns that are part of the creation of a digital dollar. This chapter also addresses whether the Federal Reserve has the authority to issue a digital currency and if a digital dollar will be *real* currency or legal tender.

The authors agree with Niall Ferguson that the introduction of the Chinese CBDC could accelerate the "demand for a monetary revolution ... [that] will be driven by digital technologies that enable not only new forms of government-issued fiat currencies ... but also private currencies generated in innovative ways, such as through distributed ledgers".[7]

Background

For over a millennium, humans have used currency as a means of exchange, a method of payment, a standard of value or a store of wealth. There are many theories about the origin of money, in part because money has many functions: it facilitates exchange as a measure of value; it brings diverse societies together by enabling gift-giving and reciprocity; it perpetuates social hierarchies; and it is a medium of state power.[8] In North America, pre-colonial Americans faced money shortages because England prohibited settlers from minting their own coins.[9] As a result, early American settlers adopted the traditional trading methods of Native Americans, who had been using goods such as wampum, furs, tobacco and maize as mediums of exchange.[10]

U.S. dollar

In 1792, the passage of the Coinage Act established the United States' first national mint, which led to the nation's first circulating coins delivered by the mint in March 1793.[11] Over the next 220 years, the concepts of currency and legal tender have evolved in the United States from coins backed by silver and gold to digital currencies built on distributed ledger technology.

Payment systems

New payment methods have developed over the centuries, including coins, banknotes, cheques, and credit cards.[12] Today, global central banks, academia, and the legal profession are actively discussing the development of CBDCs. The discussions have focused on whether the CBDCs should be issued as a retail or wholesale instrument.

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.[13] As noted by Goldman Sachs in a note to clients:

> In its most basic form, the blockchain records ownership of bitcoin and transactions involving the crypto currency across a wide network of computers, as opposed to a centralized ledger. Transactions are signed off by the parties involved using the software, checked by the network or the 'crowd', then added to the blockchain – a long string of code that records all activity. Encryption in the software ensures these 'blocks' cannot be tampered with or altered. And the decentralized nature means the 'crowd' police the whole system. The software cuts out the need for a 'trusted middleman' to sit in between parties in a transaction, such as a bank or clearinghouse. This makes transactions quicker, cheaper, and easier when compared to the current systems banks use.[14]

Many firms in the financial services industry believe blockchain technology can be adapted for use in traditional financial services transactions in a way that "has the potential to redefine transactions and the back office of a multitude of different industries. From banking and payments to ... trade settlement ... a distributed shared ledger has the potential to make interactions quicker, less-expensive and safer".[15]

Permissionless networks

On a public (permissionless) blockchain, access to the network is unrestricted. Despite public misconceptions of the technology, public blockchains are not anonymous. Users in a permissionless blockchain network use a pseudonym. On a public blockchain network, users can validate transactions. Validation is the process that ensures that all nodes are synchronised and that there is agreement on the legitimacy of transaction blocks. Consensus must be reached after each new block is added, and only after that can the block be considered immutable.[16]

Permissioned networks

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. In addition, someone must (determine and) validate cybersecurity requirements, and decide when to upgrade and validate the code.[17]

Wallets and keys

Digital assets are stored by associating them with addresses called "wallets", which can be stored on web servers, local hardware such as personal computers, jump drives and mobile devices, or on paper printouts. A digital asset wallet takes the form of a cryptographic public key, which is a string of numbers and letters. Each public key has a matching "private key", known only to the user. 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.[18]

CBDCs

At the end of 2019, central banks representing a fifth of the world's population reported that they were likely to issue CBDCs in the near future.[19] The number of central banks that are likely to issue a retail CBDC over the next couple of years doubled in 2019, to 20%.[20] By October 2020, 80% of surveyed central banks indicated that they are engaging in research, experimentation or development of CBDCs. The interest in CBDCs appears to have been fuelled by the COVID-19 pandemic. Eighty-one countries that represent over 90% percent of global GDP are now exploring a CBDC. In May 2020, only 35 countries were considering a CBDC.[21] A January 2021 report by the Bank for International Settlements indicated that of the 65 central banks surveyed in 2020 regarding their interest in CBDC, over 55 of them were exploring general purpose (i.e., retail) CBDC, of which 15 have either launched, piloted or are in the very advanced stages of exploring CBDCs.[22] Safety measures such as social distancing, public concerns that traditional currencies may transmit the COVID-19 virus, and new government-to-person payment schemes have accelerated the use of digital payments.

CBDC is central bank-issued digital money denominated in the national unit of account that represents a liability of the central bank. If the CBDC is intended to be a digital equivalent of cash for use by end users (households and businesses), it is referred to as a "general purpose" or "retail" CBDC. As such, it offers a new option to the public for holding money. CBDC is different from cash, as it comes in a digital form unlike physical coins and banknotes. CBDC is also different from existing forms of cashless payment instruments for consumers such as credit transfers, direct debits, card payments and e-money, as it represents a direct claim on a central bank, rather than a liability of a private financial institution.

Retail CBDC

A retail CBDC would be a digital liability of a central bank that can be used by the public. A retail CBDC instrument would not be commercial bank money, credit cards, or mobile payment application balances because it would be a liability of the central bank. A retail CBDC would be different from traditional currency because it would only exist in digital form.[23]

Wholesale CBDC

Wholesale CBDC is a digital liability of a central bank that is limited to certain financial institutions and is not available to the general public.[24] Wholesale CBDC is designed for use by financial institutions and is similar to traditional central bank reserve and settlement accounts.[25]

Account-based *v.* token-based

A CBDC is a digital payment instrument, denominated in the national unit of account, that is a direct liability of the country's central bank.[26] CBDC can be account-based or token-based, the former involving the transfer of a claim on an account and the latter of a token between digital wallets.[27] A transaction in account-based CBDC would entail the movement of currency based on the transfer of a claim from one account to another and would resemble transactions typically occurring between commercial bank depositors, except the accounts would be held with the central bank.[28] Accordingly, a payer would access its account at the central bank and request a transfer of funds to a recipient's account also at the central bank, with the central bank ensuring settlement by updating a master ledger after verifying the payer's authority to use the account, sufficient funds in the payer's account, and the identity and authenticity of the payee's account.[29]

A token-based CBDC would involve the transfer of an asset from one wallet to another; physical cash and many digital assets are examples of a token-based currency. More importantly, a token-based CBDC would rely on the ability of the payee to verify the validity of the CBDC.[30] With cash, the worry is counterfeiting while, digitally, the worry is whether the token is genuine and whether the token has already been spent.[31]

Centralised *v.* decentralised

A central bank's ledger for a CBDC system can be centralised or decentralised. A centralised ledger would require an intermediary to manage and transfer the liabilities.[32] In this case, the central bank likely would serve as the intermediary and be the controller of token distribution or account management. Accordingly, the central bank would take on the role of the validator for the technology that facilitates the distribution of the CBDC. In an account-based system, centralisation would mean that the central bank would serve as the administrator of all accounts and would take on the responsibility of verifying all account holders.

A decentralised ledger refers to a system where the central bank delegates responsibility to other parties. In a token-based system, third parties (such as commercial banks) would replace the central bank as validators within the technology infrastructure that facilitates the transfer and validation of CBDC-based transactions. In an account-based system, decentralisation involves third parties that are responsible for managing user accounts.

CBDC models in development

As of July 2021, there are five pioneering jurisdictions that have either fully launched a CBDC or have launched a pilot, including China.[33] Fourteen other countries, including major economies like Sweden and South Korea, are now in the pilot stage with their CBDCs

and preparing a possible full launch.[34] Nearly all of the G20 countries are in some stage of development of a CBDC. There is no uniformity as to the reasons why central banks are exploring CBDC; some are exploring CBDCs in the hope of bringing more investors to their financial system, while others are concerned about the growth of non-government sponsored digital currencies and the potential impact of those private currencies on monetary policy. Several governments, including China, may view CBDCs as a potentially powerful surveillance tool.[35] Finally, other countries including the United States view CBDCs as a tool to promote financial inclusion. The CBDC projects in Sweden, Canada, and China are instructive examples of the efforts of central banks in this area.

Sweden

The first publicly announced work on retail CBDCs was conducted by the Swedish Riksbank, the world's oldest central bank.[36] In Sweden, cash use has been declining in recent years, and the Riksbank has initiated a societal discussion on access to a central bank payment instrument for the general public. Sweden is a highly digital economy and so cash use has been on the decline for some years, to the extent that an increasing number of shops are no longer accepting cash at all. Noting that its economy is witnessing "the greatest and fastest decline in cash worldwide",[37] the Riksbank was at the global forefront of discussing the possibility of issuing a CBDC.[38]

Currently, Sweden is developing a proof of concept of the e-krona project.[39] The CBDC will be intended as a complement to, not a replacement for, cash.[40] Over time, this "e-krona" project has been further developed. In February 2020, the Riksbank announced that it would conduct a pilot project with Accenture aimed at developing a proposal for a technical solution for an e-krona.[41] The e-krona will offer the general public continued access to state money, but in digital form in an effort to promote safer and more efficient payment systems as more and more persons no longer use cash as a means of payment.[42] In May 2021, Sweden moved forward with a trial of its CBDC between its central bank and a live retail bank chain, Handelsbanken, based in Sweden.[43]

The architecture of the current Riksbank proof of concept is a hybrid CBDC. The CBDC is a direct claim on the Riksbank and payments are operated by payment service operators. The ongoing pilot is a "decentralised database of all ekronor in circulation at any given moment, where the Riksbank verifies all transactions before completion".[44] The infrastructure and technical implementation are based on the Corda blockchain developed by R3. The e-krona is focused on the domestic market, and retail use by non-residents will only occur via the use of pre-paid cards by tourists for small purchases.

Canada

The Bank of Canada has done an extensive amount of work on digital currencies. Canada was one of the first countries to explore the development of a CBDC. The Bank of Canada has not indicated that it is developing a retail CBDC,[45] but Canada has identified the conditions under which it would develop a CBDC[46] and also described possible designs.

The Bank of Canada has considered scenarios in which (i) the use of physical cash is reduced or eliminated altogether, and (ii) a private cryptocurrency makes substantial inroads as a means of payment. The Bank of Canada is engaging in discussions with stakeholders, universities, and firms on the design of a CBDC. The overall aim of the design of the CBDC is a digital claim on the Bank of Canada that closely mimics the properties of physical cash. The CBDC would not replace cash, but is rather designed as a digital addition with advantageous resilience and accessibility features.[47]

The Bank of Canada is exploring three potential models: (i) a direct CBDC (the Bank of Canada providing the entire CBDC payment system); (ii) a hybrid CBDC (the Bank of Canada only issuing and redeeming CBDC, with private sector intermediaries providing end user services); and (iii) the intermediated CBDC (identical to the hybrid model, where the Bank of Canada does not have access to the full ledger of retail transactions). The Bank of Canada is also exploring a hybrid option in which intermediaries execute the majority of payments, but the Bank of Canada can conduct some retail payments.[48]

China

China was the first leading economy to explore CBDCs, including general purpose CBDCs. The CBDC being developed by the People's Bank of China ("PBC"), the Digital Currency Electronic Payment ("DC/EP"), is the most advanced CBDC project. The DC/EP is currently being offered in four cities in China. DC/EP is available to the public and foreign visitors, and functions like cash as a liability of the PBC.[49] The PBC has been working on the DC/EP since 2014, though it released few details until 2018.[50]

The DC/EP is a centralised, digital currency issued by the PBC and is expected to be primarily used for retail payments in China.[51] China is positioning the DC/EP for international use and designing it to be untethered to the global financial system, where the U.S. dollar has been primary currency for transactions since World War II.[52] Since April 2020, this system is being tested in the context of a large-scale pilot and has not been revealed countrywide to the approximately 1.4 billion Chinese citizens but, instead, is open to selected entities in the whole country.[53] The pilot is continuously being expanded to allow an increasing number of households, banks, companies, merchants, etc. into the infrastructure.[54] In contrast to other CBDCs, the DC/EP is not based on a distributed ledger, but provides capabilities to build distributed ledger technology applications on top of the centralised infrastructure. On April 20, 2020, a PBC spokesperson confirmed that pilot testing was under way in several cities – Shenzhen, Suzhou, Chengdu, Xiong'an, and the "2022 Winter Olympics Office Area" in Beijing.[55]

In China, the introduction of a CBDC should be seen in the context of a highly digitised economy and widespread use of private digital payment services. The backbone of the DC/EP's infrastructure would be a mixed system with conventional database and blockchain. The PBC has emphasised that blockchain is not yet sufficiently mature for such a large-scale application. To settle transactions, any system has to be able to accommodate 300,000 transactions per second to accommodate the large retail transactions in China.[56] The PBC has taken steps to enable the use of DC/EP in cross-border transactions. Aiming for broad circulation in 2022, the PBC and the Hong Kong Monetary Authority began "technical testing" for use of the DC/EP in April 2021. China has conducted more than $5 billion in DC/EP transactions.[57] The PBC has also announced that it will allow foreign visitors to use DC/EP in the lead-up to the 2022 Winter Olympics. It appears that foreigners will need to provide passport information to the PBC and/or private payment service providers in order to use DC/EP, but will not need a Chinese bank account.[58]

U.S. CBDC – A day late and a digital dollar short

Unlike China, which has launched a pilot CBDC, the United States is *exploring* the potential legal and regulatory issues associated with the creation of a digital currency. "Of the countries with the largest central banks (the US Federal Reserve, the European Central Bank, the Bank of Japan, and the Bank of England), the United States is *furthest behind* [in the development of a CBDC]."[59] Earlier this month, the European Central Bank announced its intention to develop a digital euro within four years.[60]

In May 2021, Federal Reserve Chair Jerome Powell announced plans to publish a discussion paper on CBDC, focusing on the *possibility* of issuing a U.S. CBDC. Chairman Powell believed that a potential CBDC would complement the use of cash and bank deposits rather than replacing them.[61] The Chairman has said that the Federal Reserve's research into CBDCs is early and exploratory, and that U.S. officials would only consider issuing a digital dollar if they believed there was a clear use and if the idea had widespread public and political buy-in.[62]

Chairman Powell has emphasised that, as the issuer of the world's reserve currency, it is more important to be right than to be first. This is, of course, a prudent approach to a complex problem. The risk, however, is that in waiting too long, the Federal Reserve will allow a fractured digital currency ecosystem to evolve in a way that does not protect privacy and security, and over time, potentially undermines U.S. interests.[63] Staff at the Federal Reserve have noted that any discussion of a U.S. CBDC will require the central bank to focus on its role as "the guardian of public confidence in money" and that a U.S. CBDC must include "a sound legal framework".[64]

Legal authority

The launch of a U.S. CBDC will require consideration of whether the issuance of a CBDC would be consistent with the Federal Reserve's mandates, functions, and powers under the Federal Reserve Act. The first issue that must be considered is whether a CBDC is a currency, legal tender, or both.[65]

Currency

All currency issued by the Federal Reserve is a valid and legal offer of payment for settling "debts" to a creditor. Specifically, 31 U.S.C. § 5103 states that "United States coins and currency (including Federal reserve notes and circulating notes of Federal Reserve banks and national banks) are legal tender for all debts, public charges, taxes, and dues". Neither the statute nor any other federal law compels an individual or private business to accept currency or coins as payment for goods and services. Private sector entities are generally free to develop their own policies on whether to accept cash, within the boundaries of any applicable state law and with appropriate notice. As the U.S. Department of the Treasury notes in its FAQ with respect to legal tender status: "For example, a bus line may prohibit payment of fares in pennies or dollar bills. In addition, movie theatres, convenience stores and gas stations may refuse to accept large denomination currency (usually notes above $20) as a matter of policy."[66]

Legal tender

Most discussions of CBDC assume that the digital currency would be treated as currency of the United States and would therefore have legal tender status. Federal law provides that U.S. coins and currency (including Federal Reserve notes and circulating notes of Federal Reserve Banks and national banks) are legal tender for "all debts, public charges, taxes, and dues".[67] Federal Reserve notes must be accepted by creditors as valid for the payment of both public and private debts. U.S. law, however, does not require a person to accept legal tender for goods or services and does not prohibit the acceptance of other forms of "money" to extinguish a debt.[68] A CBDC's recognition as legal tender would not guarantee its acceptance in commercial use. Acceptance of a CBDC would depend on the credibility of the CBDC, including the soundness of the legal framework underpinning it (for example, commercial law rules that facilitate market activities).[69]

Monetary and financial stability

Central banks have a common mandate for facilitating monetary and financial stability to ensure a safe and sound financial system. Although policies and regulations to achieve this mandate may be idiosyncratic to the jurisdiction, every central bank observes three foundational principles when considering the issuance of a CBDC in their jurisdiction:[70]

- **Do no harm** – New forms of money supplied by the central bank should continue supporting the fulfilment of public policy objectives and should not interfere with or impede a central bank's ability to carry out its mandate.
- **Coexistence** – Different types of central bank money – new (CBDC) and existing (cash, reserve or settlement accounts) – should complement one another and coexist with private money (commercial bank accounts).
- **Innovation and Efficiency** – Without continued innovation and competition to drive efficiency in a jurisdiction's payment system, users may adopt other, less safe instruments or currencies.

Depending on the design and structure of a CBDC, its introduction into the financial system may lead to broad, macroeconomic effects.

A potential by-product of widespread adoption of CBDC in a country is the risk of bank disintermediation, particularly during times of economic stress. In the current environment, a run on central bank money could occur in the form of consumers holding more cash but such runs seldom occur given the existence of deposit insurance and bank resolution frameworks designed to protect, among other persons, retail depositors.[71] In spite of the consumer protections in place, however, it is not uncommon for the general public to shift behaviour and seek out other financial institutions (e.g., larger banks) or financial instruments (e.g., U.S. treasuries) perceived to be safer during periods of financial stress. The existence of a CBDC could facilitate "digital runs" towards the central bank because, even with presence of deposit insurance, CBDCs would almost always be the safer alternative.[72] The presence of such a safe alternative, the incentive to run away from traditional financial institutions and towards the central bank, may increase with the introduction of a CBDC.

The rapid rise and adoption of digital assets such as Bitcoin, Ethereum and even certain stablecoins globally, and the widespread adoption of non-CBDC digital assets, could weaken a country's ability to affect monetary policy and support financial stability. In an increasingly digital economy, cash likely will wane in importance and use, and payment systems may increasingly centre around social and economic platforms rather than a bank's credit provision, which could weaken traditional channels of monetary policy, particularly if a country's national currency is substituted for another currency, whether a privately created digital asset or the CBDC of another country.[73] By offering a CBDC itself, a central bank could shield its country from the proliferation of alternative units of account.

Data privacy

Unlike China's CBDC, which is believed to be structured in such a way that the government has complete control over, and line of sight into, the ledger, a U.S. CBDC should not offer the same level of transparency without suitable legal safeguards.[74] While the precise privacy-related designs of a U.S. CBDC are yet unknown, it would very likely not permit the same sort of access to personal transaction information as the Chinese CBDC.

The development of a U.S. CBDC will require central banks to consider the protection of personal data. Depending on the design of the CBDC and the role of the central bank in the arrangement, a central bank that creates a CBDC will have access to an unprecedented

amount of user and transaction information. The introduction of a U.S. CBDC will require policymakers to address questions about privacy and how personal and transactional data is stored, shared, used, and protected from unauthorised access. Policymakers will need to consider the CBDC in the context of the existing data privacy laws.

CBDC and the Federal Reserve System

On August 13, 2020, the Federal Reserve Bank of Boston announced a *multiyear* collaboration with the Digital Currency Initiative at the Massachusetts Institute of Technology ("MIT") to perform technical research related to a CBDC. The research project is focused on exploring the use of existing and new technologies to build and test a hypothetical digital currency platform.[75] The Boston Federal Reserve and MIT have structured the research collaboration into work phases that extend over two to three years. The first phase involves jointly building and testing a hypothetical CBDC for widescale, general purpose use. The objective in this phase is to determine how to architect a scalable, accessible cryptographic platform to meet the needs of a theoretical U.S. CBDC, including stringent design requirements for speed, security, privacy and resiliency.[76] In later phases, researchers will assess technology trade-offs by coding and testing various architectures, to see how they impact the CBDC's design goals. The research results will be published jointly with MIT, and the code will be licensed as open-source software, so anyone can use or continue experimenting with it.[77] In parallel to the work with researchers at MIT, the Boston Fed will independently evaluate other systems to understand their potential pros and cons in supporting a CBDC.[78]

Conclusion

The United States appears to be at least four to seven years behind China in the development of a CBDC. China's planned expansion of the DC/EP and the potential for it to be expanded to include a wholesale application present a substantial potential risk to the continuing position of the U.S. dollar as the global reserve currency. Once China has made the DC/EP available to its citizens and once it makes a wholesale version available as part of China's Belt and Road Initiative, it will have the ability to offer favourable exchange rates to all users of the DC/EP outside of China. The global use of the DC/EP will likely weaken the status of the U.S. dollar as the global reserve currency.

Equally concerning is the fact that, unlike other nations that are currently exploring CBDCs, China has not demonstrated a level of commitment to the privacy rights to its citizens in a manner comparable to the protections offered in other countries including the United States. The expansion of the DC/EP as a global currency will create a mechanism by which the Chinese government could capture massive amounts of information about users of the currency in countries around the world. Should China elect to sell securities, including Chinese government and corporate debt securities using the DC/EP, or permit the DC/EP to be used to purchase equity securities, the amount of information that could be gathered on purchasers by the Chinese government *could* be a threat to the global economy and U.S. national security.

The issuance of a CBDC requires extensive planning and a firm understanding of the potential legal, economic, social, and political effects of such action. It is understandable that countries such as the United States are taking a judicious approach with respect to the development of CBDCs. However, a measured approach should be balanced against the fact that several countries, most notably China, are in advanced stages in the development

of a CBDC. Countries that have traditionally played a leading role in the development of the global financial system are behind countries that are pursuing the development of CBDCs and may therefore risk a diminished role in the global economy. The United States can take meaningful action on the development of a CBDC and to continue its leadership role in the development of the global monetary system and the global economy.

* * *

Endnotes

1. Sir Winston Churchill.
2. Jonnelle Marte, "*Fed's Powell: China's approach to digital currency would not work in U.S.*", Reuters (April 28, 2021), *available at:* https://www.reuters.com/business/feds-powell-chinas-approach-digital-currency-would-not-work-here-2021-04-28/.
3. Senator Elizabeth Warren, "*Warren Delivers Remarks on Digital Currency*" (June 9, 2021), *available at:* https://www.warren.senate.gov/newsroom/press-releases/at-hearing-warren-delivers-remarks-on-digital-currency.
4. Andrew Ross Sorkin, "*Reading Between the Lines: A Conversation With Janet Yellen*", New York Times (Feb. 23, 2021), *available at:* https://www.nytimes.com/2021/02/23/business/dealbook/janet-yellen-dealbook.html.
5. IMF Staff, "*Digital Money Across Borders: Macro-Financial Implications*", IMF, 2020; IMF Staff, "*Casting Light on Central Bank Digital Currency*", IMF, SDN/18/08; IMF Staff, "*A Survey of Research on Retail Central Bank Digital Currency*", WP/20/104, *available at:* https://www.imf.org/en/Publications/Policy-Papers/Issues/2020/10/17/Digital-Money-Across-Borders-Macro-Financial-Implications-49823.
6. Dion Rabouin, "*The U.S. Is Losing the Global Race to Decide the Future of Money – and It Could Doom the almighty Dollar*", Time (Sept. 21, 2021), *available at:* https://time.com/6099105/us-china-digital-currency-central-bank/.
7. Niall Ferguson, "*50 Years After Going Off Gold, the Dollar Must Go for Crypto*", Bloomberg (Aug. 15, 2021), *available at:* https://www.bloomberg.com/opinion/articles/2021-08-15/niall-ferguson-nixon-the-gold-standard-and-a-bitcoin-bonanza.
8. Chapurukha Kusimba, "*When—and why—did people first start using money?*", The Conversation (June 19, 2017), *available at:* https://theconversation.com/when-and-why-did-people-first-start-using-money-78887.
9. Jeff Desjardins, "*The History of Money in America: From Beads to Virtual Currency*", (June 6, 2016), *available at:* https://www.visualcapitalist.com/the-history-of-money-in-america-from-beads-to-virtual-currency/.
10. *Id*.
11. United States Mint, "*The History of the U.S. Circulating Coins*", *available at:* https://www.usmint.gov/learn/history/us-circulating-coins.
12. Curzio Giannini, "*The Age of Central Banks*", London: Edward Elgar (2011), *available at:* https://www.e-elgar.com/shop/usd/the-age-of-central-banks-9780857932136.html.
13. Andrea Pinna, "*Distributed ledger technologies in securities post-trading*", European Central Bank (April 2016) ("Pinna") (April 2016), *available at:* https://www.ecb.europa.eu/pub/pdf/scpops/ecbop172.en.pdf.
14. Goldman Sachs, "*Emerging Theme Radar What if I Told You...Themes, Dreams, and Flying Machines*" (Dec. 2, 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...,to%20creating%20a%20%20%20alternative%20to%20fossil%20fuel%20in.

15. *Id.*
16. Pinna.
17. *Id.*
18. Richard B. Levin and Kevin Tran, "*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.
19. Codruta Boar, "*Impending arrival – a sequel to the survey on central bank digital currency*", Bank for International Settlements (Jan. 2020), *available at:* https://www.bis.org/publ/bppdf/bispap107.pdf.
20. Raphael Auer, "*Rise of the central bank digital currencies: drivers, approaches and technologies*", Bank for International Settlements (Aug. 2020) ("Auer"), *available at:* https://www.bis.org/publ/work880.pdf.
21. Atlantic Council, Central Bank Digital Currency Tracker (2021) ("Atlantic Council"), *available at:* https://www.atlanticcouncil.org/cbdctracker/.
22. Codruta Boar and Andreas Wherli, "*BIS Papers No. 114—Ready, steady, go? – Results of the third BIS survey on central bank digital currency*", Bank for International Settlements (Jan. 2021), *available at:* https://www.bis.org/publ/bppdf/bispap114.pdf.
23. Robleh Ali and Neha Narula, "*Redesigning digital money: What can we learn from a decade of cryptocurrencies?*", Digital Currency Initiative, MIT Media Lab (2020), *available at:* https://static1.squarespace.com/static/59aae5e9a803bb10bedeb03e/t/5e28b4bca9d3422148400c95/1579726012763/Redesigning+digital+money_++What+can+we+learn+from+a+decade+of+cryptocurrencies_%281%29.pdf.
24. *Id.*
25. Morten Bech, Jenny Hancock, Tara Rice, and Amber Wadsworth, "*On the future of securities settlement*", Bank for International Settlements (Jan. 2020), *available at:* https://www.bis.org/publ/qtrpdf/r_qt2003i.pdf.
26. Bank for International Settlements, "*Central Bank Digital Currencies: Foundational Principles and Core Features*" (2020) ("BIS CBDC 2020"), *available at:* https://www.bis.org/publ/othp33.pdf.
27. Charles M. Kahn and William Roberds, "*Why Pay? An introduction to payments economics*", Journal of Financial Intermediation 18(1) (Jan. 2009), *available at:* https://www.sciencedirect.com/science/article/abs/pii/S1042957308000533.
28. Tommaso Mancini-Griffoli, Maria Soledad Martinex Peria, Itai Agur, Anil Ari, John Kiff, Adina Popescu and Celine Rochon, IMF, "*Casting Light on Central Bank Digital Currency*", *available at:* https://www.imf.org/en/Publications/Staff-Discussion-Notes/Issues/2018/11/13/Casting-Light-on-Central-Bank-Digital-Currencies-46233.
29. *Id*.
30. BIS CBDC 2020.
31. *Id.*
32. *Id*.
33. Jonas Gross, "*Which Jurisdictions Head up the Retail Central Bank Digital Currency League Table*", Medium (July 27, 2021), *available at:* https://jonasgross.medium.com/which-jurisdictions-head-up-the-retail-central-bank-digital-currency-league-table-4938a996613f.
34. Atlantic Council.
35. Julia Friedlander, "*The Promises and Perils of Central Bank Digital Currencies*", House Committee on Financial Services - Subcommittee on National Security, International Development and Monetary Policy (July 27, 2021) ("Friedlander"), *available at:*

https://www.atlanticcouncil.org/commentary/testimony/friedlander-testifies-to-house-committee-on-financial-services-regarding-us-leadership-for-central-bank-digital-currency-development/.

36. The Riksbank's e-krona project – Report 1 (Sep. 2017) ("Riksbank"), *available at:* https://www.riksbank.se/globalassets/media/rapporter/e-krona/2017/rapport_ekrona_uppdaterad_170920_eng.pdf.
37. *Id.*
38. Cecilia Skingsley, "*Should the Riksbank issue e-krona?*" (Nov. 16, 2016), *available at:* https://www.bis.org/review/r161128a.pdf.
39. Payments in Sweden 2020 – Digital money – the Riksbank's e-krona pilot (Oct. 29, 2020) ("Riksbank 2020"), *available at:* https://www.riksbank.se/en-gb/payments--cash/payments-in-sweden/payments-in-sweden-2020/3.-the-riksbank-is-adapting-to-a-changing-world/digital-money--the-riksbanks-e-krona-pilot/e-krona--a-digital-complement-to-cash/.
40. Auer.
41. *Id.*
42. Riksbank e-krona project, *available at:* https://www.riksbank.se/en-gb/payments--cash/e-krona/.
43. Benjamin Pirus, "*Sweden moving forward in e-krona CBDC trials*" (May 28, 2021), *available at:* https://cointelegraph.com/news/sweden-moving-forward-in-e-krona-cbdc-trials.
44. Auer.
45. *Id.*
46. *Id.*
47. *Id.*
48. *Id.*
49. *Id.*
50. *Id.*
51. Deutsche Bank, "*Digital yuan: what is it and how does it work?*" (July 14, 2021), *available at:* https://www.db.com/news/detail/20210714-digital-yuan-what-is-it-and-how-does-it-work?language_id=1.
52. James T. Areddy, "*China Creates Its Own Digital Currency, a First for Major Economy*", Wall Street Journal (April 5, 2021), *available at:* https://www.wsj.com/articles/china-creates-its-own-digital-currency-a-first-for-major-economy-11617634118.
53. Working Group on E-CNY Research and Development of the People's Bank of China, "*Progress of Research & Development of E-CNY in China*" (July 2021), *available at:* http://www.pbc.gov.cn/en/3688110/3688172/4157443/4293696/20210716145846918 71.pdf.
54. *Id.*
55. Jess Cheng, Angela N. Lawson, and Paul Wong, "*Preconditions for a general-purpose central bank digital currency*", Federal Reserve Board (Feb. 24, 2021), *available at:* https://www.federalreserve.gov/econres/notes/feds-notes/preconditions-for-a-general-purpose-central-bank-digital-currency-20210224.htm.
56. Auer.
57. Evelyn Cheng, "Foreign travelers will be able to use the digital yuan, central bank say", CNBC (July 16, 2021), *available at:* https://www.cnbc.com/2021/07/16/pboc-foreign-travelers-to-china-will-be-able-to-use-digital-yuan.html.
58. Friedlander.
59. Atlantic Council and Friedlander.

60. For a discussion on the digital euro and the motivations of the ECB, *see* Marc-Olivier Strauss-Kahn, "*A Digital Euro*", Atlantic Council (accessed Sept. 20, 2021), *available at:* https://www.atlanticcouncil.org/economy-business/a-digital-euro/. *See* "*Eurosystem launches digital euro project*", European Central Bank (July 14, 2021), *availableat:* https://www.ecb.europa.eu/press/pr/date/2021/html/ecb.pr210714~d99198ea23.en.html.
61. Jerome Powell, "*Federal Reserve Chair Jerome H. Powell outlines the Federal Reserve's response to technological advances driving rapid change in the global payments landscape*" (Press release) Federal Reserve Board of Governors (May 20, 2021), *available at:* https://www.federalreserve.gov/newsevents/pressreleases/other20210520b.htm.
62. Jeanna Smialek, "*Jerome Powell says the Fed won't issue a digital currency without congressional approval*", New York Times (Mar. 22, 2021), *available at:* https://www.nytimes.com/2021/03/22/business/jerome-powell-says-the-fed-wont-issue-a-digital-currency-without-congressional-approval.html.
63. Friedlander.
64. Cheng.
65. Some critics of CBDCs have argued that the Federal Reserve and the U.S. Treasury do not have the constitutional authority to issue a digital currency. Paige Pidano Paridon, "*Legal Authority to Issue a U.S. Central Bank Digital Currency*", Bank Policy Institute (June 9, 2021), *available at:* https://bpi.com/legal-authority-to-issue-a-u-s-central-bank-digital-currency/.
66. *Available at:* https://www.treasury.gov/resource-center/faqs/currency/pages/legal-tender.aspx.
67. 31 U.S.C. § 5103.
68. U.S. Treasury, "*Legal Tender Status*" (2011), *available at:* https://www.treasury.gov/resource-center/faqs/currency/pages/legal-tender.aspx (noting that there is no requirement that legal tender currency or coin be accepted for payment).
69. Cheng.
70. BIS CBDC 2020.
71. *Id*.
72. *See also* Committee on Payments and Market Infrastructures—Market Committee, "*Central Bank Digital Currencies*" (Mar. 2018), *available at:* https://www.bis.org/cpmi/publ/d174.pdf ("CPMI-MC 2018").
73. Markus K. Brunnermeier and Harold Hames, "*The Digitalization of Money*" (Aug. 2019), *available at:* https://scholar.princeton.edu/sites/default/files/markus/files/02c_digitalmoney.pdf.
74. Critics of China's CBDC have raised concerns that it "will likely enable the Chinese Communist Party (CCP) to strengthen its digital authoritarianism domestically and export its influence and standard-setting abroad. By eliminating some of the previous constraints on government data collection of private citizens' transactions, DCEP represents a significant risk to the long-held standards of financial privacy upheld in free societies". Yaya J. Fanusie and Emily Jin, "*China's Digital Currency - Adding Financial Data to Digital Authoritarianism*", Centre for a New American Security (Jan. 26, 2021), *available at:* https://www.cnas.org/publications/reports/chinas-digital-currency.
75. *Id.*
76. *Id*.
77. *Id*.
78. *Id*.

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

Richard B. Levin is chair of the FinTech and Regulation Practice. He has been advising FinTech clients on legal and regulatory issues since the start of electronic trading in the late 1990s and was one of the first lawyers to focus on the regulation of blockchain and digital assets. Richard is considered a thought leader in the FinTech and regulatory space.

His practice focuses on the representation of early stage and publicly traded companies in the FinTech space, including investment banks, broker-dealers, investment advisers, peer-to-peer lending platforms, digital currency trading platforms, alternative trading systems, exchanges, and custodians. Richard represents these firms before regulators in the United States and abroad. He has been recognised by *Chambers* as a leading FinTech attorney in the Blockchain and Cryptocurrencies category since the inception of the category.

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

Kevin R. Tran 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.

Nelson Mullins Riley & Scarborough LLP

101 Constitution Avenue, NW, Suite 900, Washington, D.C., 20001, USA
Tel: +1 202 689 2800 / URL: www.nelsonmullins.com

U.S. federal income tax implications of issuing, investing and trading in cryptocurrency

Pallav Raghuvanshi & Mary F. Voce
Greenberg Traurig, LLP

Introduction

Cryptocurrency is often issued in an initial coin offering ("**ICO**") as "coins" or "tokens". Broadly, tokens can be classified as "utility tokens", which provide users with (i) access to the blockchain platform developed by the issuer, or (ii) products or services provided by the issuer on the blockchain platform, or as "security tokens", which represent certain rights with respect to an entity, either as equity or debt. Furthermore, there are so-called "intrinsic" or "convertible" cryptocurrencies that generally are used as a medium of exchange (*e.g.*, Bitcoin, Litecoin, etc., and, if permitted, Libra) or give access to a platform on which other blockchain projects are built (*e.g.*, Ether, Neo, Eos, etc.). Some cryptocurrencies, such as Ether, can be viewed as hybrid tokens that can be used as a medium of exchange for ICOs of other cryptocurrencies, but also allows smart contracts for other blockchain projects to be built on its platform.

This chapter is intended as a primer on certain U.S. federal income tax implications of cryptocurrency transactions and structures. The Internal Revenue Service ("**IRS**") provided its first official guidance in Notice 2014-21,[1] which generally described the U.S. federal income tax treatment of cryptocurrencies. Subsequently, in October 2019, the IRS issued Rev. Rul. 2019-24[2] and a frequently asked questions ("**FAQ**") document providing additional guidance on the tax treatment and reporting obligations for transactions involving cryptocurrencies. Because of the limited authority directly on point, much of the discussion below is based on analogies to the tax treatment of other property where the rules are more developed or on the application of the language of statutory provisions, regulations, and other authorities.

Notice 2014-21: In general

The basic rule of Notice 2014-21 is that cryptocurrency is property for U.S. federal income tax purposes and not "currency". Therefore, taxpayers may not use cryptocurrency as a functional currency for purposes of Internal Revenue Code ("**IRC**" or "**Code**") Section 985, and transactions in cryptocurrency would never be Section 988 transactions.[3] Further, the rules applicable to foreign currencies do not apply to transactions in cryptocurrencies.[4]

More troubling for taxpayers is that, if cryptocurrencies are property, every disposition of cryptocurrency is a disposition of property. Each time cryptocurrency is purchased for fiat currency (such as U.S. dollars), basis must be recorded and tracked, and each time a chunk of cryptocurrency is disposed of, gain or loss is recognised.[5]

One problem with Notice 2014-21 is that it appears to be limited by its terms to what we would call "cryptocurrency", rather than to utility tokens or equity tokens. It seems to apply only to cryptocurrency that can be used to pay for goods or services or that is held

for investment purposes, and focuses on cryptocurrency that has an equivalent value in fiat currency, or that acts as a substitute for fiat currency (referred to as "convertible" cryptocurrency). However, since logic dictates that utility tokens and equity tokens also should be treated as property, the remainder of this chapter assumes that all tokens are property and not money and discusses U.S. federal income tax issues only unless otherwise indicated.

Initial coin offerings/first token sales

Startup companies may use ICOs as a means of raising funds. An ICO is the issuance of newly generated tokens for other cryptocurrencies or, less commonly, for fiat currency. Issuers can offer non-functional tokens, the proceeds from which are used by the issuer to develop its platform, product or services. Once the platform or product is fully functional, token purchasers can use the tokens for accessing the platform, product or services developed by the issuer. Alternatively, unless token purchasers are subject to a "lock-up" period, they can be exchanged for other tokens or fiat currency.

Less commonly, companies issue tokens that represent an ownership interest in the company or other property, or that are intended simply as a means of exchange.

Tax implications of ICOs for U.S. issuers

In general

The issuance by a U.S. issuer of utility or convertible tokens for cash, tokens, or other property may be treated as a sale (or, potentially, a license) of property or a promise to perform services in the future. As discussed below, in many of these situations, a domestic issuer will recognise income upon the issuance of the tokens or, potentially, later, when the services are performed.

Character and source of income

The U.S. tax implications to the issuer of tokens depend on whether income from their issuance will be characterised as sales, royalty or services income, and on the source of such income (*i.e.*, the jurisdiction in which it arises for U.S. tax purposes).

In 1998, the IRS issued Treas. Reg. § 1.861-18 (also known as the "**Software Regulations**"), which provide a framework for determining the character of income from the transfer of intangible property. Although the Software Regulations were issued long before blockchain technology was even contemplated, they logically can be used as a starting point for determining the character and source of income from a cryptocurrency transaction.

Under such regulations, income from the transfer of intangible property is classified as: (1) the sale of copyright rights; (2) the license of copyright rights; (3) the sale of a copyrighted article; (4) the lease of a copyrighted article; (5) the provision of services related to a computer program; or (6) the provision of know-how related to a computer program.[6]

(a) Treatment of transfer of tokens as a sale

Generally, the issuance of tokens should not result in the transfer of copyright rights because token purchasers generally do not acquire unfettered rights with respect to the underlying blockchain technology. While tokens can provide the right and ability to build upon a blockchain platform, this right would appear to be more in the nature of a service or a licence rather than a right to prepare a derivative work. For example, creating a private blockchain on the Ethereum platform requires the installation of "Geth". A private blockchain created with Geth is a new asset facilitated by Ethereum, but is not a derivative of Ethereum.

However, the issuance of tokens might be analogised to a sale of intangible property that has indicia of a copyrighted article in that the purchaser acquires all of the benefits and burdens of an asset (*i.e.*, a token) that are separate from the underlying blockchain platform and that can be used in perpetuity.[7] In that case, the character of the income from the sale of a token will depend upon the character of the token in the hands of the transferor. It is unlikely that newly issued tokens qualify as capital assets in the hands of the issuer. Since newly issued tokens are created with the intention of selling them, they could be viewed as inventory.

If the tokens are inventory and were "produced" by the issuer, such income would be sourced based on the location of production of such inventory.[8] However, the place of "production" of the tokens might not be at all clear. In a situation where the tokens are issued based on open-source technology, with all of the actual development to come afterward, the jurisdiction of the issuer might be the place of production. However, the place where the concept was created or tested or where the programmers sit might be a more realistic alternative.

(b) Treatment as a licence

The issuance of a token could, to some extent, be viewed as including a licence to use the issuer's blockchain platform (*e.g.*, to access content on the platform or to build a separate blockchain project keyed off the issuer's blockchain intellectual property ("**IP**"), although this might also be viewed as a service (as discussed below)).[9] To the extent the issuance is treated as a licence, the amount received for the tokens would be considered a royalty, which would be ordinary income, and the source of the royalty would be the place where the token is used, which may not be easily determined.[10]

(c) Treatment as a service

Potentially, the consideration received for the issuance of tokens could be treated as compensation for the provision of services provided by the issuer.

This treatment could apply to pre-ICO tokens where the issuer accepts consideration from the investors subject to an obligation to use the consideration to develop the issuer's technology, although the issuer's efforts generally would be considered services only if the token holders would have an ownership interest in the IP that is developed, which is unlikely in most cases.[11] Any income from services would be ordinary income and generally would be sourced to the location where the services are performed.[12] Services performed by individuals generally are sourced to the place where they are located when the services are performed.[13] If equipment is involved in the performance of services, the location of the equipment is also considered.[14]

A blockchain platform may also provide automated services by acting as an online intermediary linking customers with providers or by hosting or streaming information or content that can be accessed by token holders. In such a case, sourcing the revenue will present more than the usual challenges for sourcing income because of the decentralised nature of blockchain technology.

Timing of recognition of income by issuers

Generally, income must be recognised immediately upon receipt of consideration for the transfer of property or the provision of services – *i.e.*, in the case of an ICO, at the time of the issuance. However, in certain limited circumstances, an accrual basis issuer can defer taxation on at least a portion of the amount received to the succeeding taxable year if the

receipt of the consideration is treated as an advance payment for future goods or services (*e.g.*, for pre-functional tokens).[15] The sale of pre-functional tokens or an agreement to sell future tokens (also known as Simple Agreement for Future Tokens ("**SAFT**")) could also potentially be viewed as a forward contract to develop the technology and deliver the functional tokens in the future. Generally, under the common law open transaction doctrine, the execution of a forward contract will not be a taxable event until the transaction is closed.[16] However, if the governing documents do not contain a refund provision, it is highly likely that the amount received by the issuer would be considered income at the time received.

Regardless of when the income is recognised, a U.S. issuer should be able to offset such income with operating losses (or depreciation or amortisation of capitalised expenses) incurred prior to issuance to the extent eligible to be carried forward. For foreign issuers, operating losses can be carried forward for use against U.S. income only if the issuer files timely and accurate U.S. income tax returns for the years in which the losses were incurred.[17]

Tax consequences to issuer of use of tokens by purchasers

Notice 2014-21 provides that a taxpayer who receives cryptocurrency as payment for goods or services must include in gross income or gross receipts the fair market value of the tokens, measured in U.S. dollars as of the date the tokens are received. Thus, if the issuer provides a service that is accessed by using tokens it had previously issued, the issuer would include, in income, the fair market value of the tokens at the time of their use (which could be offset by the issuer's cost of providing the services). The issuer's tax basis in the tokens received in exchange for the services would be the fair market value of the tokens at the time of their receipt.

Tax implications for token purchasers in an ICO

Purchase of tokens

The purchase of tokens in an ICO using fiat currency should not be a taxable event for the purchaser. However, if tokens are purchased using another cryptocurrency, a U.S. taxpayer would recognise gain or loss equal to the difference between the value of the tokens purchased and the tax basis in the cryptocurrency exchanged therefor.

A purchaser's basis in the tokens acquired would be their purchase price in U.S. dollars (or translated into U.S. dollars at the time of purchase if purchased using another cryptocurrency).

Sale or use of tokens

If tokens are subsequently sold or transferred in exchange for goods or services, the transaction generally will be a taxable event and will give rise to capital gain or ordinary income depending on their character in the hands of the token holder. The amount of the gain or loss will be the difference between the token holder's basis in the tokens sold or exchanged and the amount of fiat currency or the fair market value of property or services received for them.[18]

If the tokens were held as an investment or for trading, then the gain or loss generally should be capital gain or loss, and would be short term or long term depending on whether the tokens were held for more than one year. If the tokens were held by an individual as personal-use property and not for investment (*e.g.*, to access media, to shop or for comparable purposes), such property would be a capital asset and any gain (but not loss) recognised on the disposition of such cryptocurrency generally would be treated as described above, except that losses would not be allowed.

Furthermore, although Notice 2014-21 is silent with respect to the use of tokens in transactions that might otherwise result in non-recognition, presumably the language in Q&A #1 to the effect that "general tax principles applicable to property transactions apply to transactions using virtual currency" would cover this situation. Accordingly, the contribution of tokens or cryptocurrency to a corporation in exchange for its stock or to a partnership in exchange for a partnership interest should not result in any gain or loss if a transfer of any other property would result in non-recognition (*e.g.*, pursuant to IRC § 351 or § 721).

If the tokens are not held as capital assets or personal-use property and do not qualify as Section 1231 assets (*e.g.*, if they constitute inventory), and do not qualify for tax-free treatment under a non-recognition provision, the token purchaser would recognise ordinary gain or loss on their sale or exchange. To date, there is no *de minimis* exception for small transactions, and a significant issue for token holders is how to determine the basis of the particular tokens used and the value of the property or services received in return.[19]

Hard forks, soft forks, airdrops and awards/rewards

The term "airdrop", as used currently in an evolving cryptocurrency jargon, means a project founder's distribution of tokens, coins or other digital assets to holders of existing cryptocurrency without any consideration from the token recipient. Generally, airdrops occur when a new blockchain project distributes free tokens to existing holders of certain cryptocurrency such as Bitcoin and Ethereum. Issuers may also issue tokens as rewards for using an app, purchasing merchandise, referring customers, watching advertisements, etc.

A "hard fork" is a material change to a blockchain-system protocol that generally (but not always) results in a split of the existing blockchain protocol pursuant to which the nodes running on the existing version of the blockchain are no longer accepted in the updated version. As a result, a new blockchain is created that follows the updated rules, while the pre-split blockchain that follows the legacy rules still exists. A holder of a pre-split cryptocurrency generally receives additional cryptocurrencies that are generated by the newly created blockchain. For example, Bitcoin hard forks that occurred in August 2017 and October 2017 created a split in the existing Bitcoin blockchain, and pre-split Bitcoin holders received Bitcoin Cash and Bitcoin Gold, respectively.

A soft fork is a backward-compatible method of upgrading existing nodes. If a majority consensus is reached for the new rules, then only the new chain is followed. In soft forks, holders may also be required to take affirmative action to get access to or convert their outdated tokens (which may be worthless) for the upgraded tokens.

Generally, a U.S. taxpayer's gross income means all income from whatever source derived,[20] and the Supreme Court defined gross income as an undeniable accession to wealth over which the taxpayer has complete dominion.[21] On October 9, 2019, the IRS released a revenue ruling (Rev. Rul. 2019-24), which generally addresses questions related to the tax treatment of hard forks. The tax treatment of the receipt of the new cryptocurrency will be based on whether the owner of the legacy cryptocurrency is able to take dominion and control over the new cryptocurrency generated as a result of the hard fork. If a taxpayer has immediate dominion and control over the new cryptocurrency, the taxpayer will be required to include in his/her gross income (as ordinary income) an amount that is equal to the fair market value of the new cryptocurrency that was transferred to his/her account/wallet and will take a basis in such new cryptocurrency equal to such fair market value. Owners of an existing cryptocurrency who do not receive dominion and control over the

new cryptocurrency at the time of the hard fork (for example, because their wallets may not be compatible to support the new cryptocurrency) will not have income at the time of the hard fork. They presumably would have income when they achieve dominion and control over the new cryptocurrency, although this is not specifically stated. Similar to hard forks, the IRS would also consider receipt of tokens by a taxpayer via airdrops or rewards as undeniable access to wealth and therefore taxable.[22]

Tokens received in hard forks, airdrops, or as rewards generally must be included in income at their fair market value. Most airdropped tokens have zero value at the time of the airdrop and will not result in any taxable income unless the taxpayer achieves dominion and control over the airdropped token only when it has more than zero value. However, tokens received in hard forks, *e.g.*, Bitcoin Cash, may have a significant value, which can be determined by looking at the price for which it is being traded on an exchange at the time the taxpayer acquires dominion over such tokens. The value of tokens received as rewards will have to be determined based on the facts.[23]

Notice 2014-21 does not provide any guidance for determining the fair market value of tokens that are not listed on an exchange. In such cases, the general rules of taxation apply, and the taxpayer must make a good faith effort to determine the value of such tokens by considering all the relevant factors. The income, if any, of a holder on the receipt of tokens in a hard fork or airdrop or as a reward should be treated as ordinary income as there is no sale or exchange of a capital asset that resulted in such accretion to wealth. The basis in the tokens received should be equal to the amount included in income.

The tax treatment of a soft fork may be different because the holder of the original tokens generally must exchange those tokens for the new tokens to preserve any value. FAQs issued by the IRS on October 9, 2019 clarified that soft forks do not result in a division of the ledger and thus, no new cryptocurrency is created in soft forks. Accordingly, the IRS concluded that soft forks should not result in any income to the taxpayer as the taxpayer will be in the same position as s/he was in prior to the soft fork.

Use of a foreign jurisdiction for token issuance

A foreign issuer generally can avoid U.S. taxation on an ICO if it avoids critical contact with the U.S. However, some or all of the income of a foreign issuer can be subject to U.S. tax to the extent the income of the issuer is sourced to the U.S., which will depend on the character of the income (sales, royalties or services), where the management of the entity is located, where decisions are taken, whether marketing activities or sales take place in the U.S., and any number of other factors. As a general rule, gain on a sale of personal property by a foreign person is sourced to the jurisdiction of the seller.[24] However, if the tokens constitute inventory in the hands of the issuer (which is likely), special rules apply. If the inventory is considered to be "produced" by the issuer, then the income is allocated and apportioned between sources within and without the U.S. based on where the "production activities" occurred.[25] This might not be readily apparent, although the location of the individuals who developed the concept, the promoters and the IP developers are logical places to start.

Notwithstanding that a foreign issuer might avoid U.S. tax on an ICO, U.S. shareholders of the foreign issuer may not be as fortunate. First, if the IP was developed in the U.S., any contribution of such IP to a foreign corporation in exchange for its stock generally will be a taxable event,[26] and, in certain circumstances, could result in a corporate "inversion" that would cause the foreign corporation to be treated as a U.S. corporation.[27] Any actual sale or license of such IP by a U.S. person to a foreign entity also would result in a taxable

event, and would be subject to the U.S. transfer pricing rules.[28] These rules require that payments between related parties for the purchase, license, lease or use of property be set at arm's length rates, which requires that the consideration received (whether as a lump sum or over time) be commensurate with the income attributable to the IP. Furthermore, income generated by an ICO or from ongoing operations of a foreign issuer that is a controlled foreign corporation ("**CFC**")[29] could give rise to Subpart F income or global intangible low-taxed income ("**GILTI**") that may be includible in the income of any direct or indirect U.S. shareholder of such CFC that owns, directly or indirectly, at least 10% of its voting power or value (a "**U.S. 10% Shareholder**"). In addition, if a foreign corporation qualifies as a passive foreign investment company ("**PFIC**"), it could generate a roster of issues for certain of its direct or indirect U.S. owners who are not caught by the CFC rules.[30]

Investing, trading and dealing in cryptocurrencies

While the dividing line is blurred, a person generally will be a trader rather than an investor in cryptocurrencies if its trading is frequent and substantial.[31] While both traders and dealers may buy and sell within a very short period of time and take advantage of cross-border price-differential arbitrage, the major distinction between dealers and traders is that dealers have "customers" to whom they are selling rather than simply non-customer counterparties. Income or loss of dealers in cryptocurrencies will be ordinary in character.

Cryptocurrencies held by an investor or a trader generally will qualify as capital assets and gain or loss from their sale or other disposition generally will constitute capital gain or loss, which will be short or long term depending on whether the cryptocurrency sold or disposed of was held for more than one year.

Source of income

As a general rule, income from the sale of personal property (other than inventory) by a U.S. resident is sourced to the U.S., and by a non-resident is sourced outside the U.S.[32]

Taxation of U.S. traders in cryptocurrencies

U.S. taxpayers who trade in cryptocurrencies may be taxable or tax-exempt (*e.g.*, individual retirement accounts or other retirements funds, charitable organisations, etc.). U.S. taxpayers who are individuals generally would be subject to U.S. federal income tax at rates graduating to a maximum of 37% in the case of short-term capital gains and ordinary income, and 20% in the case of long-term capital gains. Such individual investors may also be subject to the 3.8% net investment income tax ("**NIIT**") on their net investment income, which is likely to include income from cryptocurrencies or a crypto fund.

U.S. taxable investors that are corporations generally would be subject to U.S. federal income tax at a flat 21% rate regardless of whether the income allocated to it is capital gain or ordinary income and regardless of its source.[33]

U.S. tax-exempt entities generally would be subject to tax on any gains from trading in cryptocurrencies only to the extent that such income is characterised as unrelated business taxable income ("**UBTI**"). For this purpose, gains and losses from dispositions of "property" are specifically excluded from UBTI unless the property is subject to acquisition indebtedness or is inventory held for sale to customers in the ordinary course of an unrelated trade or business.[34] Cryptocurrency is classified as "property" for tax purposes. Therefore, assuming an exempt entity is a trader or invests in a fund that is a trader in cryptocurrencies and does not otherwise hold cryptocurrency for sale to customers, its gain might not be treated as UBTI.[35]

Taxation of foreign traders in cryptocurrency

The U.S. taxation of non-U.S. traders in cryptocurrencies depends on whether the income earned is characterised as income that is effectively connected with a U.S. trade or business ("**ECI**") or investment income.

ECI

Trading in stock, securities or commodities constitutes a trade or business for U.S. income tax purposes and, if such activities are carried on in the U.S., they generally will generate ECI. However, there is a limited exception to ECI treatment for gains and losses that qualify for the "Trading Safe Harbor" under IRC § 864(b)(2). Under that provision, foreign persons that trade in stock, securities or commodities (and derivatives based on stock, securities or commodities) in the U.S. *for their own account* are not considered to be engaged in a U.S. trade or business. Such trading can be done in the U.S. by the taxpayer through its own personnel or through a resident broker, commission agent, custodian, or other agent.[36]

The principal issue for foreign traders in cryptocurrencies is that cryptocurrencies, with limited exceptions, will not qualify as stock, securities or commodities for U.S. tax purposes. The definition of a security for tax purposes is very different than for securities law purposes, and includes only stock in a corporation, interests in widely held or publicly traded partnerships or trusts, and notes, bonds, debentures, or other evidences of indebtedness,[37] and it appears unlikely that most types of cryptocurrency could qualify as securities under any of these categories. To qualify as a commodity, a cryptocurrency would have to be listed on commodity exchanges located in the U.S., such as the CME or the CBOE, and not constitute goods or merchandise that are traded in "ordinary commercial channels".[38]

The IRS has issued a private letter ruling involving foreign currencies, which are also treated as "property" for U.S. tax purposes, in which it took the position that in order for trading in a foreign currency to qualify for the Trading Safe Harbor, the *specific* foreign currency in which the trading occurred had to be traded on a commodities exchange.[39]

Bitcoin derivatives are currently traded on exchanges that are regulated by the Commodity Futures Trading Commission, and trading activity in Bitcoin or Bitcoin derivatives (but not in other cryptocurrencies) may therefore qualify for the Trading Safe Harbor.[40]

Notwithstanding that income from trading in cryptocurrencies may not qualify for the Trading Safe Harbor, if a trader operates from outside the U.S. (*i.e.*, if the trader is an individual, such individual, or if the trader is an entity, its personnel, are located outside the U.S., decisions are taken outside the U.S. and trades are placed outside the U.S.), it should not be considered to be engaged in a U.S. trade or business, and thus should not be taxable by the U.S. except to the extent that the income from such trading is derived by a U.S. citizen or resident that otherwise is subject to U.S. taxation.

Investment income

Gain or loss from the sale by a foreign individual or entity of cryptocurrency that is held as an investment should not be subject to U.S. tax as it should qualify as capital gain or loss and be sourced to the country of the foreign seller. Again, however, U.S. members of such an entity may be subject to U.S. tax if, *inter alia*, the entity is a partnership or other form of tax-transparent entity, or if the U.S. anti-deferral rules applicable to CFCs, PFICs, etc., apply.

Endnotes

1. 2014-16 IRB 938, 03/25/2014.
2. 2019-44 IRB 1004, 10/09/2019, IRC Sec(s). 1001.
3. IRC § 988(c)(1).
4. Notice 2014-21 Q&A #2.
5. This is complicated by the fact that lots of cryptocurrencies are not fungible. Each time a taxpayer disposes of a lot of, *e.g.*, Bitcoin, the specific lot or lots must be specified in the block. It would be welcome relief if future IRS guidance provides that a simplified accounting method, such as FIFO or LIFO, could be used.
6. Treas. Reg. § 1.861-18(c).
7. *See* Treas. Reg. § 1.861-18(c)(ii).
8. IRC § 863(b).
9. It is also possible that some states may take the position that if it is treated as a licence to use Software as a Service ("**SaaS**") or Platform as a Service ("**PaaS**"), it might be subject to sales and use tax under existing state sales tax rules (for states that tax such services).
10. IRC § 861(a)(4).
11. IRC §§ 861(a)(3), 862(a)(3).
12. IRC § 861(a)(3).
13. IRC §§ 861(a)(3), 862(a)(3).
14. *See*, *e.g.*, *Comm'r v. Hawaiian Philippine Co.*, 100 F2d 988 (9th Cir. 1939), cert. denied, 307 U.S. 635; Piedras Negras Broadcasting Co., 43 BTA 297 (1941).
15. IRC § 451(c).
16. *See*, *e.g.*, Rev. Rul. 2003-7; *Estate of Andrew J. McKelvey, et al. v. Commissioner*, 148 T.C. No. 13 (Apr. 19, 2017).
17. IRC § 882(c); Treas. Reg. § 1.882-4(a); *Swallows Holding, Ltd. v. Commissioner*, 515 F.3d 162 (3d Cir. 2008).
18. *See* Notice 2014-21 Q&A #5.
19. Notice 2014-21 Q&A #13 specifically provides that a person who, in the course of a trade or business, makes a payment using virtual currency worth $600 or more in a taxable year to an independent contractor for the performance of services is required to report that payment to the IRS and to the payee on Form 1099-MISC.
20. IRC § 61.
21. *See Commissioner v. Glenshaw Glass*, 348 U.S. 426, 431 (1955).
22. *See*, *e.g.*, Treas. Reg. § 1.61-14(a); *Cesarini v. U.S.*, 296 F.Supp. 3 (N.D. Ohio 1969); *Hornung v. Commissioner*, 47 T.C. 428, 1967 (T.C. 1967); *Haverly v. United States*, 513 F.2d 224 (7th Cir. 1975).
23. Perhaps the IRS will see fit to treat tokens received as rewards like frequent flying miles and not assert that such rewards are income unless and until further guidance is provided. *See* Announcement 2002-18, 2001-CB 621.
24. IRC § 865(a).
25. IRC § 863(b).
26. IRC § 367.
27. IRC § 7874.
28. IRC § 482.
29. A CFC is a foreign corporation owned more than 50% (by vote or value) by U.S. persons, each of whom owns directly, indirectly or by attribution at least 10% (by vote or value) of such corporation.
30. IRC §§ 1291–1298.

31. *See*, *e.g.*, *Ball v. Commissioner*, T.C. Memo. 2000-245; *Mayer v. Commissioner*, T.C. Memo. 1994-209; *Holsinger v. Commissioner*, T.C. Memo. 2008-191.
32. IRC § 865(a).
33. *See* IRC § 7201 *et seq*. for tax consequences of not reporting the income.
34. IRC § 512(b)(5).
35. IRC § 512(b)(1).
36. Treas. Reg. § 1.864-2(c).
37. IRC § 475(c)(2).
38. Treas. Reg. § 1.864-2(d)(3).
39. PLR 8326013, Dec. 27, 1982.
40. In *Commodity Futures Trading Commission v. McDonnell*, No. 1:18- cv-00361 (Mar. 6, 2018), a New York federal judge ruled that cryptocurrencies can be regulated by the CFTC.

Pallav Raghuvanshi
Tel: +1 212 801 2151 / Email: raghuvanship@gtlaw.com

Pallav Raghuvanshi focuses his practice on U.S. and international tax matters in the context of corporate restructurings and cross-border mergers and acquisitions. He is experienced in handling spin-off transactions for large multinational companies, various inbound and outbound transactions involving issues related to foreign tax credits, tax treaties, controlled foreign corporations, and other international reorganisation issues. He also handles U.S. federal tax aspects of initial coin offering/first token sales and other tax-related issues on blockchain technology and cryptocurrencies.

Mary F. Voce
Tel: +1 212 801 6878 / Email: vocem@gtlaw.com

Mary F. Voce concentrates her practice on corporate and international tax. She handles both inbound and outbound corporate and international tax planning for U.S. and foreign corporations, U.S. federal taxation of partnerships, limited liability companies, funds and joint ventures. She also handles U.S. federal tax aspects of cross-border corporate mergers, acquisitions and reorganisations, taxation of real estate investments, securities offerings by U.S. and foreign corporations, international projects, equipment leasing and financing.

Greenberg Traurig, LLP

MetLife Building, 200 Park Avenue, New York, NY 10166, USA
Tel: +1 212 801 9200 / URL: www.gtlaw.com

Raising capital: Key considerations for cryptocurrency companies

David Lopez, Colin D. Lloyd & Laura Daugherty
Cleary Gottlieb Steen & Hamilton LLP

Most cryptocurrency companies see numerous opportunities for growth and entry into new markets. As an owner or a management team, you may be considering funding those growth opportunities from sources that go beyond crypto tokens and into the private or public capital markets. These sources may include a private placement, initial public offering ("IPO"), acquisition by a special-purpose acquisition company ("SPAC"), or direct listing. Each option has differing strengths and weaknesses, which this chapter surveys.[1]

Cryptocurrency companies seeking to access the capital markets for the first time should keep a few things in mind:

- The requirements for an offering of securities that are evidenced by book-entry or physical certificates are a known quantity. The requirements for offering securities using distributed ledger or blockchain technology are still evolving. Careful planning will be needed if you wish to go this route.
- Capital markets investors vary widely in their sophistication and knowledge of the crypto space. You should be prepared to explain your business and financials in some detail, in slide decks, presentations or more formal written offer material.
- The preparation of these materials takes time, so appropriate advance planning is important. The involvement of a mix of disciplines can add value to the process, including representatives from your strategy, finance, legal and accounting groups.
- Equally important, the content of the materials must be accurate and not misleading, as required by U.S. securities laws. You may be liable to investors if your content does not comply with these rules. Consultation with experienced counsel will help you avoid this risk.
- Financial intermediaries, such as investment banks or placement agents, can help identify and solicit investors, as well as advise you on crafting a compelling marketing story. However, they also face requirements to know the company, its business and its personnel, which must occur before onboarding you as a client or assisting with a securities transaction. You should plan in advance, together with your advisors, for the "due diligence" review they will conduct.
- Each funding source mentioned above has pros and cons. To determine which is right for you, you will want to consider whether your team is ready to begin life as a public company (and comply with ongoing public company obligations), how valuable it is to give current shareholders the opportunity to resell or to gain "currency" to use to retain employees or make acquisitions, what cost you are willing to bear in connection with the transaction, and the speed with which you require funding, among other considerations.

Can I finance my company through digital asset securities?

While many cryptocurrency companies may envision issuing a digital asset security rather than a traditional security utilising a centralised clearinghouse, such an approach presents unique challenges. There is no clear guidance from the U.S. Securities and Exchange Commission (the "SEC") or the Financial Industry Regulatory Authority ("FINRA")[2] regarding how exchanges, broker-dealers and other intermediaries are to treat digital asset securities, particularly in regard to custody, clearing and settlement.

The guidance that does exist essentially prevents any full-purpose broker-dealers from providing these services for digital asset securities. Given the integral role that broker-dealers play in the capital markets, these evolving rules substantially limit the liquidity of digital asset securities.

What information do I need to provide to prospective investors?

The amount and type of information you will need to provide to investors will depend on the type of capital raise you wish to pursue. Private placements are relatively more flexible, with the content of offering materials being driven largely by marketing needs (*i.e.*, investors) and having relatively less detail, while IPOs, direct listings and, to some extent, de-SPAC transactions are more structured, having specific regulatory disclosure requirements and requiring relatively more detailed offering materials.

Regardless of the level of detail, most offering materials will contain at least the following: (i) a business description; (ii) a summary of strengths and strategies; (iii) financial data (potentially with audited historical financial statements); and (iv) a description of the attendant risks of an investment in your company. The due diligence process is often used to flesh out and verify the contents of the offering materials.

Why is the due diligence process an important consideration?

Due diligence is a key part of any private or public financing transaction. Investors conduct diligence for the practical purpose of evaluating both the opportunity and the risk of an investment in an enterprise. Financial intermediaries need to understand the opportunity and risk profile so they can adequately assess and explain it to investors on your behalf. Financial intermediaries are also motivated to protect themselves from reputational, regulatory and liability risk. For example, financial intermediaries will focus on the quality and scope of your company's compliance function because, as regulated entities, they would suffer reputational damage and regulatory scrutiny if they were to be associated with a capital raise for a company that is later found to be deficient in this area.

Financial intermediaries (and issuers) are also motivated to conduct diligence and vet the contents of any offering materials. This is because they have potential liability if investors suffer a loss and their investment decision was motivated by materially inaccurate statements or misleading omissions in the "story" the company gave them during the marketing of the deal. Financial intermediaries that can show, in a public offering, that they conducted "due diligence" and had a reasonable belief in the accuracy of the offering materials or, in a private offering, that they did not act "recklessly", will be safeguarded from disclosure liability under securities laws.

There are well-worn paths for the diligence review that financial intermediaries and, in most private offerings, investors pursue in any financing transaction. However, cryptocurrency

companies present unique regulatory due diligence issues, and a crypto company is well served to anticipate these inquiries and lay the groundwork to provide acceptable answers and documentation.

What will regulatory diligence focus on?

Among other items, investors may wish to see evidence of compliance, such as copies of licences, as well as policies and procedures to mitigate regulatory risks. Investors may also wish to speak with key personnel at the company regarding compliance. Key regulatory issues for cryptocurrency companies that are likely to be considered during due diligence include the following:

Securities Laws: A risk faced by cryptocurrency companies is the potential that they are impermissibly transacting in securities. For example, one or more of their prior cryptocurrency offerings may have inadvertently been a securities offering that was not in compliance with U.S. securities laws, or they may have allowed securities to trade on their platform. Such a determination would matter to investors because it would have broad regulatory (and, in turn, operational) implications. This is because offers or sales of securities must be registered or exempt, and many securities intermediaries, such as exchanges and broker-dealers, are required to register with the SEC.[3]

The lack of clear regulatory standards for determining whether a digital asset is a security limits the ability of cryptocurrency companies to ensure they are not transacting in securities, and exposes them to second-guessing by the SEC and private plaintiffs. Consultation with counsel can help to mitigate this risk by ensuring that you are aware of and avoid legal foot faults. Investors may also wish to review legal advice a company has received and speak with its outside counsel on these issues.

Investment Company Act of 1940/Investment Advisers Act of 1940: At first blush, most readers may reflexively skip this paragraph because of the assumed inapplicability of investment company regulation (which is usually associated with mutual funds or other similar enterprises) to a crypto company. Unfortunately, the definitions of "investment company" and "investment adviser" are broader than intuition would indicate, and the SEC has recently indicated particular interest in this area in relation to stablecoins.

Classification as an investment company or an investment adviser triggers a comprehensive regulatory scheme, including operating restrictions (including, in some cases, restrictions on the ability to issue debt) and registration and reporting requirements that would make continued operation cumbersome. Both of these topics are important to discuss with your legal advisors so that, if needed, your business model can be adjusted to avoid these classifications and the ensuing regulation and restrictions.

Commodities Regulation: The regulatory authority of the U.S. Commodity Futures Trading Commission (the "CFTC") extends to derivatives products, and the CFTC has begun instituting enforcement actions against both fraudulent and manipulative actors in virtual currency spot markets and against persons operating as unregistered regulated entities and intermediaries.

Putting aside fraud and other bad acts, companies should be aware that the CFTC has issued guidance expansively defining the scope of derivatives it regulates, especially in the case of leveraged or margined transactions involving retail investors, and has aggressively pursued cases involving even seemingly minor instances of wash trades and undisclosed proprietary trading in the spot markets. In order to avoid wrongdoing, it is helpful for crypto companies to develop and implement policies addressing matters regulated by the CFTC.

Anti-Money Laundering: Regulatory risks for cryptocurrency companies also include non-compliance with Bank Secrecy Act of 1970 regulations for money services businesses, state money transmitter licensing requirements, state crypto regulatory regimes and anti-money laundering ("AML") laws and regulations, among others. In addition to concerns about the cryptocurrency company's compliance, investors, particularly banks, may be concerned with the possibility that an investment may compromise their own compliance (*e.g.*, banks must ensure compliance for their own AML obligations with respect to use of proceeds). Regulations applicable to financial institutions also open up companies to potential reputational and legal exposure, such as if criminals were discovered to operate through a crypto exchange. Given the difficulties associated with satisfying AML obligations in a decentralised global market, cryptocurrency companies can be expected to make significant investments in people and technology to mitigate these risks.

Privacy Law: Improper safeguarding of customer or other personal data may lead to privacy law compliance concerns. Cryptocurrency companies should be aware that privacy laws may impose broad requirements, and may apply outside the borders of the country that promulgated the law (*e.g.*, the European Union's General Data Protection Regulation 2016/679 applies to non-European Union establishments if they are doing business with people located in the European Union).

Cybersecurity: Cryptocurrency companies are also at risk of operational harm from cybersecurity hacks, breaches or other incidents, as well as the risk of regulatory non-compliance, such as failing to obtain a required licence. Cybersecurity is a key area of disclosure focus not only for investors, but for the SEC. You should ensure that cybersecurity risks, including any past incidents, are properly disclosed to investors and presented in the offering document in order to protect against disclosure liability.

Tax: Tax risk includes the failure to remit or withhold proper taxes, which may lead to reputational risk as a "tax dodger", as well as the possibility of enforcement actions. There is little guidance about taxation of cryptocurrencies, and that which does exist is largely unfavourable to taxpayers and therefore should be carefully navigated. Cryptocurrency companies should seek to remain apprised of developments in this space and ensure compliance with any changes.

Other Areas: While we have provided a summary of some of the key regulatory issues that may be emphasised during the due diligence process, there are many other regulatory-related areas that may become a focus of due diligence. These include commercial and insolvency law treatment, custodial risk, competition and antitrust, political, legislative and regulatory responses and consumer protection concerns. You should be aware of the broad nature of the due diligence process and be prepared to produce materials and answer questions on a wide range of regulatory topics.

What does non-regulatory due diligence look like?

In addition to the regulatory due diligence discussed above, a private or public capital markets financing will also likely include:

Financial and Business Due Diligence: Financial and business due diligence is typically handled at a "management due diligence" session including senior management, during which the issuer, banks and their counsel review and discuss historical financial information, operations, current business, business plans, projections and other data.

Documentary and Legal Due Diligence: Documentary and legal due diligence includes review by lawyers of key corporate documents, including internal corporate documents

(articles, minutes and resolutions), material contracts, auditors' litigation letters and, where relevant, materials relating to intellectual property (licences, patents and trademarks). In many private and public securities offerings, lawyers deliver a negative assurance, or "10b-5" letter, stating that nothing has come to their attention that would lead them to believe that the disclosure document contains a material misstatement or omission. This 10b-5 letter is a key part of how financial intermediaries build their due diligence defence.

Accounting Due Diligence: Accounting due diligence includes discussions with the company's financial team and auditors of the company's financial statements, the audit process and related matters. In many private and public securities offerings, the company's auditors deliver a "comfort letter" to the financial intermediaries confirming their independence (a requirement in public transactions) and that they have examined and confirmed certain financial numbers included in the offering document.

Should I issue equity, debt or convertible securities?

A key question at the outset of any capital markets financing transaction is what sort of security to issue. Equity is often attractive to start-ups because it provides permanent financing without need for repayment, with the trade-off of selling a piece of the economics and, for voting securities, control of the company.

Traditional debt is less popular with start-up companies due to the need to pay interest and repay principal. Further, if the company is not yet able to show consistent EBITDA generation, the debt markets may be unreceptive or may require a set of contractual limitations on the company's operating activities (ability to incur debt, make distributions to owners, etc.), which are intended to protect creditors.

Convertible debt may be of interest, as the ability of holders to convert into equity is an option with value and significantly lowers the interest rate on the debt. However, the equity when converted may be dilutive, as it may be at a discount to the company's valuation at the time of conversion.

What deal types are available to raise capital?

Common capital markets financing deal types include: (i) private placement; (ii) IPO; (iii) acquisition by a SPAC; and (iv) direct listing.

What is a private placement and what are the key considerations?

Under the Securities Act of 1933, all offerings of securities must be registered with the SEC or be structured to take advantage of an exemption from registration. A private placement is one such exemption[4] that allows offers and sales of securities, but only to a limited set of investors with minimum levels of sophistication and knowledge. Investors who are typically permitted to purchase securities in private placements include: (i) "accredited investors" (including entities with assets exceeding $5 million or individuals with assets exceeding $1 million or earnings over $200,000 annually); (ii) "qualified institutional buyers" (also known as "QIBs", meaning institutions that own or invest at least $100 million of securities and certain other institutional investors); and (iii) investors outside of the U.S.

Typical private placement transactions include sales of minority equity stakes directly to investors or through financial intermediaries, venture capital funding rounds and broader offerings to multiple institutional, accredited and non-U.S. investors. Securities issued in a private placement cannot be listed on U.S. exchanges such as the New York Stock Exchange (the "NYSE") or NASDAQ, though they are often listed in other jurisdictions

such as Luxembourg, Singapore or Ireland. Private placement securities are sometimes issued with registration rights, which allows the issuer to issue unregistered securities now with a promise to register the securities with the SEC in the future.

Pros: A private placement is faster and cheaper than a traditional IPO because the SEC does not review and comment on the offering documentation. Further, correctly implemented private placements do not trigger SEC reporting obligations, which are costly.

Cons: Securities sold in a private placement do not have a ready resale market and will be subject to securities law limits on transferability. These facts may limit liquidity for the investors.

Key Players: The key players involved with a private placement depend on the type of private offering. For example:

- **Placement Agent**: More likely to be seen in a "true" or "traditional" private placement to a small group of investors, a placement agent is a registered broker-dealer that connects investors with companies offering securities and can offer substantial advice in the preparation of offering materials.
- **Issuer's Auditor**: The auditor aids the issuer in the preparation of financial statements and delivers comfort letters to financial intermediaries.
- **Counsel**: Counsel is typically barred in the state of New York, as many capital markets offerings are done under New York law, but may also include local counsel in jurisdictions where the issuer operates. Counsel plays various roles and, in some cases, delivers to the placement agent a 10b-5 letter and aids in the preparation of offering documentation and related contracts.

What is an IPO and what are the key considerations?

An IPO refers to a traditional, underwritten and SEC-registered IPO. Because the securities are registered, they may be sold broadly to the public, and they are not subject to the same restrictions on transfer as unregistered securities sold in a private placement. Securities issued in a traditional IPO are typically listed on a U.S. exchange such as the NYSE or NASDAQ.

Pros: An IPO is a traditional and prestigious way to access the capital markets. An IPO provides an opportunity to raise capital (through a primary offering) as well as an opportunity for existing shareholders to sell as desired (through a secondary offering).

As compared to a direct listing, a benefit of an IPO is that underwriters assist with marketing the offering to a large number of potential investors, which helps to achieve widespread distribution of the securities and leads to a ready and liquid market for future fundraises. Underwriters in an IPO also support aftermarket trading. At pricing, a traditional IPO may achieve a very favourable price-earnings multiple.

Cons: An IPO is a more expensive and lengthy process than a private placement. Preparation of the registration statement typically takes one to two months and requires significant attention from management and the company's lawyers and auditors. It also requires an SEC review and comment process, which can take months to complete, as well as the payment of SEC registration fees.[5] Other processes, such as due diligence, are also typically more elaborate compared to a private placement.

An IPO also brings with it a more elaborate regulatory landscape, including ongoing corporate governance, internal control over financial reporting and SEC disclosure requirements, such as annual (10-K), quarterly (10-Q) and periodic (8-K) reports made available to the public via the SEC.

Disclosure Document: The key disclosure document for an IPO is called a "registration statement", and within the registration statement is the prospectus. Unlike the offering material in a private placement, the registration statement is filed with the SEC and is available to the public. This is a comprehensive document that explains the business, risks and financial condition of the issuer, as well as the structure of the security issued, among other topics. The contents of the registration statement are mandated by SEC rules and regulations, as well as by exchange rules and market practice. The registration statement must include two years[6] of historical financial statements audited in accordance with U.S. GAAP for domestic companies. Any interim financial statements may be unaudited but must be subject to limited review by auditors and must comply with SEC requirements.

Shareholder Considerations: Underwriters require that existing shareholders and employees enter into lock-ups that typically restrict them from selling their securities before 180 days after the IPO.

Certain shareholders of the company, which frequently include founders, directors and officers, are required to report their ownership publicly via the SEC's EDGAR platform, among other requirements. Shareholders that are required to report their ownership include beneficial owners of greater than 5% of the public company's equity, directors and officers. Directors, officers and owners of more than 10% of the company's equity must generally disgorge any "short-swing" profits realised from purchases and sales of the issuer's equity securities within six months of each other.

Key Players: Many of the players in an IPO are the same as those in a private placement, although there are some differences.

- **Underwriters**: Underwriters enter into an "underwriting agreement" with the issuer to purchase the securities upon issuance and aid in marketing and the preparation of the prospectus. Typically, there are one to three lead banks, or "bookrunners", that lead the underwriting syndicate, advise the issuer on valuation and offering structure, build a book of orders and price the offering. Additional banks are typically called "co-managers".
- **Issuer's Auditor**: The auditor must be independent and not perform prohibited non-audit services.
- **Counsel**: In addition to its role in a private placement, counsel assists in navigating and managing the SEC process.
- **Independent IPO Advisor**: There is a growing trend towards retaining an independent IPO advisor to provide strategic advice and help assess input from lead underwriters.

Multi-Class Structure: Multi-class structure, or dual-class structure, refers to an architecture where a company has two or more classes of stock with disparate voting rights. The "high vote" class may be given to founders or other key owners to provide an outsized voice in the direction of the company. Examples of companies with a multi-class structure include Blue Apron, Snap, Facebook, Alphabet and Alibaba. If a company is interested in implementing a multi-class structure, it should do so as part of its IPO.

Proponents of multi-class structure argue that it insulates management and certain shareholder classes from "short-termism" forces. The main downsides of a multi-class structure are that it may have a potential impact on pricing due to critical investor reaction, and it is unpopular with institutional investors, proxy advisory firms and certain indices. A multi-class structure can be unwound if no longer desired.

What does it look like to be acquired by a SPAC and what are the key considerations?

Acquisition by a SPAC is a popular option for cryptocurrency companies – more popular than a traditional IPO.

A SPAC is a shell company that raises money from investors in the public markets to fund its acquisition of a private company. The SPAC conducts an IPO shortly after its formation and attracts investors based largely on the reputation of its sponsor and management team. The SPAC sells shares to the public, typically in a "unit" coupled with a fraction of a warrant that allows the shareholder to purchase a share of the SPAC's stock at a certain price and time. The proceeds from the IPO are placed in a trust account. The SPAC searches for and acquires a private operating company, and funds this acquisition with the IPO proceeds and additional private placements, if needed. This acquisition is referred to as the initial business combination ("IBC") or "de-SPAC". Once the SPAC has acquired a target, the target company becomes an SEC-reporting, publicly traded company.

Pros: Acquisition by a SPAC provides access to liquidity and potential access to key talent with the right SPAC sponsor team. There is less execution uncertainty when compared to a traditional IPO, as the price and terms are negotiated in private before committing. There is flexibility to negotiate terms not achievable via a traditional IPO (*e.g.*, the ability to have an earn-out for management and target shareholders).

Cons: You cannot control whether you will locate a SPAC that is interested in acquiring your company. There is potential for dilution from the privately placed SPAC securities held by the SPAC sponsors (which are referred to as the "promote", and usually equivalent to 20% of the total outstanding shares of the SPAC).

After the de-SPAC, the target becomes a public company that is subject to the same reporting obligations and increased public scrutiny as a company that elected to go public via a traditional IPO. Because SPACs are typically required to complete an IBC within 24 months and the de-SPAC process typically takes only three to five months, the target company must swiftly implement public company architecture, including that related to internal controls and audit matters, tax matters, human resources, technology and cybersecurity, and prepare audited financials to be filed during the de-SPAC process.

De-SPAC Process: Once a SPAC has selected its target, they enter into merger negotiations, beginning with diligence. Unlike capital markets diligence, de-SPAC diligence may require non-disclosure agreements, have an added focus on contract provisions important in the context of the sale of a company (such as change of control provisions), and may include extra work to prepare schedules and memorandums reflecting the diligence conducted.[7]

The SPAC and the target then negotiate a merger agreement, which is ultimately filed with the SEC. The target and the SPAC likewise line up private investment in public equity, or "PIPE", investors, who typically sign up at the same time that the merger agreement is signed. It is during these negotiations that the post-merger capital structure, funding and governance are decided.

SPAC Shareholder Approval: The SPAC shareholders must approve the IBC. While most IBCs are approved, this adds an additional layer of uncertainty.

Ability of Target Affiliates to Sell Shares: Shares of a SPAC-target-turned-public-company cannot be sold by a holder that was an "affiliate" of the target company (as determined prior to the de-SPAC) for the first year after the de-SPAC except in (i) an SEC-registered transaction, or (ii) a private resale in which the buyer takes restricted securities. After the first year, current or recent affiliates of the listed company need to comply with limitations and requirements of Rule 144 under the Securities Act to resell securities to the public outside of a registered transaction.

De-SPAC transactions often require the listed company to file a resale shelf to be used by PIPE investors and target shareholders that would not otherwise be able to freely resell. This registration statement is subject to SEC review, meaning that there will be a gap between its filing and the commencement of the public offering.

Key Players: In addition to auditors and counsel, SPAC key players include:

- **Sponsors**: The sponsors are the founders of the SPAC. The term "sponsor" is also often used to refer to the privately held entity that holds the SPAC's promote shares on behalf of the founders.
- **SPAC Investors**: SPAC investors include public shareholders, as well as institutional anchor or forward purchase investors. Institutional investors may have special incentives, such as a share of the promote or influence in target selection.
- **M&A Advisors**: A de-SPAC is at its heart an M&A transaction. Both the SPAC and the target typically retain legal and financial M&A advisors in addition to capital markets counsel.

What is a direct listing and what are the key considerations?

A direct listing is a specialised type of IPO whereby the issuer lists its stock directly on a securities exchange without the involvement of an underwriter. Once the registration statement becomes effective, the issuer becomes a publicly reporting company and shareholders are able to sell (subject to some limitations).

Pros: A direct listing offers a degree of liquidity to existing shareholders without subjecting them to an IPO-style lock-up and without requiring the company to raise additional capital in the process (which may be a pro or a con, depending on your capital needs). A direct listing is seen as a highly transparent process, particularly in regard to its market-driven pricing structure, and may also generate press due to its relative rarity. It has the potential to be faster than a traditional IPO.

Cons: A direct listing realistically requires strong name recognition for success. In a traditional IPO, underwriters help introduce the issuer to major mutual funds and other investors; without underwriters, some observers have asked whether the audience of potential buyers and valuation may be more limited than in a traditional IPO. Direct listings may not create the liquid market that a traditional IPO creates, which in turn may result in thin trading and increased price volatility. In a traditional IPO, underwriter support helps generate liquidity and analyst coverage for the securities from the outset, as coverage is typically bundled into the standard IPO book-building process. While well-known companies, such as Spotify and Slack, that have elected the direct listing route have enjoyed substantial analyst coverage, smaller issuers may not.

As in a traditional IPO and a SPAC acquisition, the end result is that the issuer becomes a public company. The issuer is therefore required to put in place public company infrastructure and to comply with SEC reporting obligations on an ongoing basis.

Comparison to Traditional IPO: Some of the key ways that a direct listing compares to a traditional IPO include the following:

- **No Underwriter**: Direct listings involve registered sales directly into the public market with no intermediary underwriter and therefore no underwriting commission (however, the issuer still must pay "advisory fees" to the banks, although these can potentially be lower than a traditional underwriting fee).
- **Price Setting**: In a direct listing, the initial price is set during the opening auction. In contrast, in a traditional IPO, the price is set by agreement between the company and the underwriter based on input and indications of interest from investors.

- **Marketing**: Direct listings do not typically involve a roadshow like in a traditional IPO. However, companies undertaking direct listing may conduct an "investor day" to present the issuer to the investor community. The company's financial advisors can be engaged to help prepare the presentations but, unlike a roadshow, will not participate in them.
- **Liquidity for Pre-IPO Shareholders**: Because direct listings are done without underwriters, they do not require existing shareholder lock-ups.

Key Players: A direct listing has many of the same players as a traditional IPO, except:

- **Financial Advisors**: In a direct listing, the banks act not as "underwriters" but as "financial advisors". The financial advisors may assist in putting together the equity story for the prospectus and investor day presentation and assist in determination of reference price (*not* a book-building). A direct listing leads to decreased work and liability for bankers.

Primary vs Secondary Direct Listing: In a primary direct listing, a company sells newly issued shares directly to the public. In a secondary direct listing, the company sells already-existing shares to the public. In both, it does so on its own behalf and directly to the public as part of its NYSE or NASDAQ listing process.

Until recently, exchange rules would only permit companies to conduct secondary direct listings. However, on December 22, 2020, the SEC approved an NYSE rule change that allows companies going public to raise capital through a primary direct listing,[8] and, on May 19, 2021, the SEC approved a parallel proposal from NASDAQ.[9] To date, no company has completed a primary direct listing and the interplay between the new stock exchange rules and existing SEC rules remains unclear.

Overview

Objective	Private Round	SPAC	IPO	Direct Listings
Raise funds to grow business	Yes	Yes	Yes	Maybe[10]
Owners can sell down interest	No	Yes	Yes[11]	Yes
Creation of "acquisition currency"	No	Yes	Yes	Yes
Preserve founders' control through dual-class structure	Yes	Yes	Yes	Yes
Attract and retain top talent	No	Yes	Yes	Yes
Market risk to execution	Less	Less	More	More
Cost	Low	High	High	Medium
Dilution	Some	High	Some	None

* * *

Endnotes

1. This chapter is focused on U.S. companies interested in the U.S. private or public capital markets.
2. FINRA is a government-authorised, not-for-profit organisation that oversees U.S. broker-dealers.

3. *E.g.*, on August 9, 2021, the SEC issued a cease-and-desist order against digital asset exchange Poloniex, Inc. for allegedly operating an unregistered exchange in violation of Section 5 of the Exchange Act of 1934 in connection with its operation of a trading platform that facilitated the buying and selling of digital asset securities. The SEC stated that Poloniex facilitated trading of "digital assets that were investment contracts and therefore securities".
4. Private placements are typically conducted under Section 4(a)(2) of the Securities Act, which exempts from registration transactions by an issuer not involving a public offering.
5. The current SEC filing fee rate is available here: https://www.sec.gov/ofm/Article/feeamt.html.
6. This chapter assumes emerging growth company ("EGC") status. If not an EGC at the time of the IPO, reporting and regulatory obligations, including around financial statements, are more onerous. In order to qualify as an EGC, a company must have total gross revenues for its most recently completed fiscal year of less than $1.07 billion.
7. A commonly repeated idea is that SPACs are low liability because they are not subject to the same disclosure requirements as a traditional IPO. However, the SEC has spoken out against this proposition. For more information, please see this public statement: https://www.sec.gov/news/public-statement/spacs-ipos-liability-risk-under-securities-laws.
8. For more information, please see the following SEC release: https://www.sec.gov/rules/other/2020/34-90768.pdf.
9. For more information, please see the following SEC release: https://www.sec.gov/rules/sro/nasdaq/2021/34-91947.pdf.
10. The stock exchanges recently changed their rules to allow direct listings with a primary issuance component. However, the SEC has not made clear in their rules how this will work. So, it is possible to raise money in a direct listing, but the first company that tries will need to work through a number of issues of first impression with the SEC, which could delay execution and cause uncertainty.
11. There may be marketing issues if the public perceives that the "smart money" is getting out.

David Lopez
Tel: +1 212 225 2632 / Email: dlopez@cgsh.com

David Lopez is a partner based in Cleary's New York office. His practice focuses on representation of corporate clients in a wide range of corporate governance, public reporting, capital markets, finance and liability management matters.

David has extensive experience with initial public offerings for domestic and foreign private issuers, public and private debt, equity and structured securities offerings for established companies and a range of liability management transactions such as issuer self-tender, exchange offers, consent solicitations and open market strategies. He has been recognised as a leader in capital markets by *Chambers Global*, *Chambers USA*, *IFLR1000*, *The Legal 500 U.S.* and *Who's Who Legal*.

David received a J.D. from the University of Chicago Law School and an A.B., *cum laude*, from Cornell University.

Colin D. Lloyd
Tel: +1 212 225 2809 / Email: clloyd@cgsh.com

Colin D. Lloyd is a partner based in Cleary's New York office. He advises on a broad range of securities and derivatives regulatory, legislative, transactional and enforcement matters. His clients include broker-dealers, swap dealers, banks, exchanges, trading platforms, clearinghouses, private equity funds, investment managers, sovereigns and derivatives end users. He is regularly counsel to leading trade associations and *ad hoc* coalitions on major industry initiatives.

Colin has been recognised by *Chambers USA*, *The National Law Journal*, *IFLR* and *Law360*. He was also one of three lawyers distinguished by the Institute of International Finance in 2015 as a "Future Leader" under 40.

Colin received a J.D., *cum laude*, from Harvard Law School and a B.A., *summa cum laude*, from Vanderbilt University.

Laura Daugherty
Tel: +1 212 225 2000 / Email: ldaugherty@cgsh.com

Laura Daugherty is an associate based in Cleary's New York office. Her practice focuses on cross-border corporate and financial transactions, principally in Latin America, and SPAC upper-tier structuring and investments.

Laura received a J.D., with honours, from the University of Washington School of Law and a B.A., *summa cum laude*, from the University of Washington.

Cleary Gottlieb Steen & Hamilton LLP

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

Smart contracts in the derivatives space: An overview of the key issues for buy-side market participants

Jonathan Gilmour & Vanessa Kalijnikoff Battaglia
Travers Smith LLP

There is no universally accepted definition for 'smart contracts', but this term is commonly used to refer to legal contracts (or elements of legal contracts) being represented and 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. Smart legal contracts would comprise pieces of smart contract code creating a legally enforceable arrangement. 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.

There has been an increased interest from key industry bodies, such as the International Swaps and Derivatives Association (**ISDA**) on the development of technology-enabled solutions (including the use of smart contracts), which will allow a fundamental reshaping of the derivatives infrastructure. The expectation is that these solutions should improve operating efficiency, reduce operating costs and risk, and increase both quality and transparency of data.

Latest developments in the derivatives market

There is still a long way to go, but some of the key developments involving ISDA's work to facilitate the use of smart contracts across the derivatives industry include:

(i) In 2017, ISDA issued the first version of the Common Domain Model (**CDM**), known as ISDA CDM 1.0, followed by its second version, ISDA CDM 2.0, which 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. ISDA has also been working to update the 2006 ISDA Definitions (including through the 2021 ISDA Interest Rate Derivatives Definitions, which are expected to be published later this year) to make them more compatible with the CDM.

(ii) On 6 October 2020, ISDA and Digital Asset (a blockchain start-up) launched a pilot implementation of the CDM for the clearing of interest rate derivatives (the **CDM Clearing Pilot**) using DAML, an open-source reference code library that is intended to facilitate the implementation of the CDM. The CDM Clearing Pilot is expected to allow a superior level of standardisation and automation of derivatives clearing processes.

(iii) 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. ISDA has produced guidance on the use of smart derivatives contracts in relation to:

- **ISDA Master Agreement** (February 2019) – the paper acts as an introduction to the ISDA 2002 Master Agreement for potential fintech developers and highlights the interdependence of key mechanics within the 2002 Master Agreement, including events of default and termination events, payment and delivery obligations, close-out and netting.
- **Collateral** (September 2019) – as parties to derivatives contracts are becoming increasingly subject to margin requirements, automation of the collateral exchange process would ease the administrative burden. ISDA proposals include automating the resolution of disputes in a timely fashion, automating the valuation of collateral and streamlining the collateral enforcement process.
- **Equity Derivatives** (February 2020) – the ISDA 2011 Equity Derivatives Definitions provide potential for broader standardisation across the market, which lends itself to the use of smart derivatives contracts. The paper proposes that automation be facilitated through pre-defined options in the Relationship Supplement or a Transaction Supplement to the Definitions. Fintech solutions based on the 2011 Equity Definitions framework offer a chance to build shared processes on a standard CDM representation.
- **Interest Rate Derivatives** (February 2020) – a key driver in the development of the revised ISDA Interest Rate Definitions has been to ensure that the standardised definitions are more technology-friendly. 'Light chain' systems would allow market participants to exchange information in relation to interest rate derivatives in a more automated way, while 'heavy chain' systems could potentially allow collateral to be transferred and held digitally.
- **Credit Derivatives** (November 2020) – credit derivatives transactions often incorporate automated functions and there remain further opportunities for greater automation and more efficient straight-through post-trade processing. The paper addresses new technology solutions to facilitate the efficiency of delivery of existing services (e.g. by aiding reconciliation or the more complex processing required in index credit default swaps) and the use of distributed ledger technology (**DLT**) or similar technology to provide for more efficient settlement in the credit derivatives market.
- **Foreign Exchange Derivatives** (November 2020) – the risks inherent in the cross-border nature of FX derivatives can be addressed through enhanced automated processes and the development of digital instruments for valuation and/or settlement. The paper sets out how the use of smart contracts and new DLT can provide scalable, cost-efficient and more accurate technology solutions within the FX market.

(iv) 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. On 25 May 2021, ISDA announced the expansion of the platform to include ISDA's collateral documentation. The database is expected to improve the efficiency of contract negotiation and facilitate the digitisation of legal documentation.

(v) On 21 January 2021, ISDA made the ISDA Master Agreement digitally available for the first time via ISDA Create. The ISDA Clause Library is also being added to the platform as part of this rollout. ISDA Create allows users to produce and agree documentation online, as well as store legal data from these documents. Originally launched in 2019 to help firms negotiate initial margin documentation to comply with the margin rules, it was extended in 2020 to a number of other documents.

(vi) On 19 March 2021, ISDA published its response to the HM Treasury Consultation and Call for Evidence on UK Regulatory Approach to Cryptoassets and Stablecoins. The response highlighted the potential benefits of the adoption of DLT and smart contracts in the derivatives market.

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, including 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.

In relation to its work in further developing the CDM, ISDA has also established a governance framework – this includes an executive committee (which oversees strategy for the adoption of the CDM) and forums of technical and product experts.

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

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

For a smart legal contract to produce its intended legal effect, its automated provisions (or smart contract codes) must be legally validated by a lawyer. This might be challenging as it would require lawyers 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 the terms in the ISDA Master Agreement (or schedule). Appropriate mechanisms for resolving any resulting 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 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 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 in the event of a cyber security incident.

For instance, smart derivatives contracts for FX or interest rate derivatives may use an external data source to determine FX or interest 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 coding error on the part of the third party.

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 post 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.

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.

What should a buy-side market participant be doing?

The market is still evolving and is in its early stages of developing a model that works across the derivatives industry. For the time being, buy-side entities should consider becoming involved with the initiatives put forward by ISDA, including the working group discussions and projects. It is also important for buy-side entities to discuss and compare notes with their peers, counterparty banks, legal advisers and other market participants on the changes that will need to be implemented into their systems and processes to allow for the use of smart derivatives contracts.

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 team. 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 2021 edition of *The Legal 500* as a "Leading Individual" in derivatives and structured products.

Vanessa Kalijnikoff Battaglia
Tel: +44 20 7295 3150 / Email: vanessa.battaglia@traverssmith.com

Vanessa Kalijnikoff Battaglia is a senior counsel in the finance department at Travers Smith, where she is part of the Derivatives & Structured Products team. Vanessa joined Travers Smith in 2014, having previously qualified to practise law in both Brazil and New York. She acts for funds, asset managers, pension schemes, fintechs and financial institutions advising on derivatives and structured products. Vanessa has contributed to a number of guidelines published by ISDA on the use of smart contracts in the derivatives space. Vanessa is described by *The Legal 500 UK* as a "very capable and commercially minded lawyer, careful with details without ever missing the big picture", and was recognised in the 2021 edition as a Rising Star.

Travers Smith LLP

10 Snow Hill, London EC1A 2AL, United Kingdom
Tel: +44 20 7295 3000 / URL: www.traverssmith.com

Tracing and recovering cryptoassets: A UK perspective

Jane Colston, Jessica Lee & Imogen Winfield
Brown Rudnick LLP

Introduction

On the one hand, the cryptocurrency market is rapidly developing, with multiple cryptocurrencies, crypto derivatives and other cryptoassets increasingly accessible and promoted. On the other hand, we see, for example, the Financial Conduct Authority's (the "**FCA**") website cautioning that "*cryptoassets are considered very high risk, speculative investments*" that will likely fall outside the remit of the Financial Ombudsman Service or the Financial Services Compensation Scheme.[1] While the law and regulation concerning cryptoassets is still in a relatively nascent state, it is adapting at pace to seek to ensure that investors are protected. For example, in January 2020, new regulatory powers were introduced to allow the FCA to supervise how cryptoasset businesses manage the risk of money laundering and counter-terrorist financing.[2] UK cryptoasset businesses must comply with the Money Laundering Regulations and register with the FCA.

As litigators, we see cryptoasset-related disputes increasing and the courts stepping in to provide meaningful remedies. We see investors swindled in various ways resulting from phishing and social media scams, ransomware attacks and fraudulent investment schemes including fake cryptocurrencies and Initial Coin Offerings ("**ICOs**"). Digital wallets and entire exchanges have also been hacked, enabling fraudsters to transfer the assets elsewhere having obtained the user's private key. To cover the fraudster's tracks, non-digital assets may be stolen and then converted into cryptocurrency. Sophisticated hackers have even manipulated the blockchain supporting cryptocurrencies and gained majority control of the network, allowing them to privately reroute transactions and double spend the assets.

The work of the UK Jurisdiction Taskforce (the "**UKJT**"),[3] chaired by Sir Geoffrey Vos, Master of the Rolls, signals that the UK is well equipped to resolve interim and underlying disputes concerning cryptoassets. As the UKJT observed in its Legal Statement on Cryptoassets and Smart Contracts (the "**Legal Statement**") of November 2019: "*The great advantage of the English common law system is its inherent flexibility… judges are able to apply and adapt by analogy existing principles to new situations as they arise.*"[4] Sir Geoffrey Vos continues to reinforce the commitment of the English judiciary to produce a legal system in England and Wales "*that embraces new technologies, and allows disputes arising from the financial markets of tomorrow to be resolved quickly and efficiently and at proportionate cost*".[5]

To assist victims of cryptocurrency fraud, the courts of England and Wales (the "**E&W Courts**") have recently confirmed the availability of various existing legal remedies such as disclosure orders (compelling third parties to produce certain information aimed at identifying fraudsters and asset tracing) and asset preservation orders (such as proprietary and freezing orders). Where assets have been transferred to on-chain wallets held by

third parties such as exchanges or custodians operating in the UK or internationally, these third parties will be key targets for information gathering. We consider this further in the "Tracing and recovering cryptoassets" section below.

So how are disputes in this digital space (including fraud claims) resolved?

Resolution of crypto-related disputes in England and Wales

There is increasing recognition within the UK legal community of the need to establish certainty around the treatment of cryptocurrency, distributed ledger technology and smart contracts (self-executing contracts run on blockchain technologies that automatically process transactions without the need for a third party) to instill confidence in their use.

The UKJT set out its authoritative Legal Statement with this objective following a consultation that revealed several areas requiring legal clarification.

In particular, and relevant to the availability of proprietary remedies in the event of crypto fraud, the Legal Statement concluded that cryptoassets are capable of having proprietary status under English law, indicating as follows:[6]

i. In principle, the law will treat cryptoassets as property where they demonstrate the characteristics of definability or certainty, identifiability by third parties, some degree of permanence or stability, and exclusivity or control.
ii. Unlike some other digital assets, cryptoassets amount to more than pure information as their commercial value is not in the recorded data but in the ability to authenticate dealings in cryptoassets pursuant to the rules of the system.
iii. Cryptoassets need not be things in possession or things in action to constitute property.[7]
iv. As with other intangible property, title to cryptoassets can be vested or transferred by assignment or agreement of the owner, and cryptoassets may be secured by a mortgage or equitable charge provided a proprietary interest has been granted.
v. Ownership of a cryptoasset will generally be demonstrated by the holder of the private key. Notable exceptions include circumstances where a private key has been unlawfully obtained, and potentially where a private key is held on another person's behalf.
vi. The general legal principle that someone may not validly transfer to someone else something they do not own is unlikely to apply to cryptoassets, as the transfer generates new code and therefore a new asset, while the original asset ceases to exist.

As discussed further below in the "Tracing and recovering cryptoassets" section, the Legal Statement was promptly endorsed by the E&W Courts as "*an accurate statement as to the position under English law*",[8] and subsequent decisions have confirmed that cryptoassets are generally regarded as property for the purposes of English law.[9]

The UKJT subsequently published its Digital Dispute Resolution Rules (the "**Rules**"), providing an alternative dispute resolution scheme for disputes concerning cryptoassets, smart contracts and blockchain applications that might otherwise be resolved by on-chain or automatic dispute resolution processes, or by alternative off-chain methods.[10] The Rules may be incorporated into contracts, digital assets or digital asset systems and provide a helpful blueprint, which parties are free to modify.

The Rules essentially provide for arbitration in a rapid timeframe, save for circumstances that the parties have agreed would be better served by expert determination. Strikingly, the outcome of any automatic dispute resolution process will be legally binding under the Rules. Arbitration under the Rules will be adapted to the circumstances of the case and could be conducted entirely electronically. An arbitral tribunal will have the power to operate, modify, sign or cancel any digital asset relevant to the dispute, or direct any party

to do so (which could be a helpful tool to circumvent enforcement where cryptoassets have been transferred unlawfully). There is scope for parties to remain anonymous from each other should they wish, and for the publication of awards to help create precedent albeit they are anonymised.

The Rules offer an additional layer of flexibility to traditional arbitration, which may appeal to those caught up in crypto-related disputes, with advantages such as confidentiality, the ability to select arbitrators with relevant expertise, and broad international recognition of agreements and awards under the New York Convention on the Recognition and Enforcement of Foreign Arbitral Awards.

The Rules make it possible, therefore, for parties to agree at the outset that disputes arising will be handled under the fast-track process the Rules envisage. Litigants, directors and insolvency practitioners need to be aware of these new Rules as they may find them written into the smart contracts to which a company is party, as follows: "*Any dispute shall be resolved in accordance with UKJT Digital Dispute Resolution Rules.*" Such a provision would assist the rapid resolution of disputes given the design of the Rules, the effect of which could be, for example, that the tribunal implements its judgment by modifying (or directing a party to modify) any digital asset relevant to the dispute.

What are the interim remedies the E&W Courts will grant to locate fraudsters and stolen cryptoassets?

Tracing and recovering cryptoassets

An asset recovery strategy will require clarity on *what* cryptoassets are the subject of the recovery, *when* cryptoassets were fraudulently stolen, *where* those cryptoassets are now and *who* was involved in the fraud.

The "*What?*": Cryptocurrency as an asset/property

On two occasions prior to the Legal Statement, the E&W Courts were prepared to treat Bitcoin as property and granted proprietary injunctions over it.[11] Since the Legal Statement, several other English court decisions have affirmed the status of cryptocurrencies as property.[12]

The New Zealand courts (the "**NZ Courts**") also reached that conclusion in *Ruscoe v Cryptopia Ltd (in liquidation).*[13] This case arose out of the collapse of a cryptocurrency exchange (Cryptopia), which was hacked. The NZ Courts had to determine the distribution of cryptocurrencies held by Cryptopia as between the account holders (who argued that these were held on trust for them by the exchange) and Cryptopia's creditors. The court found that cryptocurrencies met the definition of property under local company law and indicated that they would likely satisfy the test under common law, considering the criteria set out by Lord Wilberforce in *National Provincial Bank Ltd v Ainsworth*:[14] definable; identifiable by third parties; capable of assumption by third parties; and some degree of permanence and stability (factors that had influenced the Legal Statement). As such, it was held that Cryptopia was not the owner of the cryptocurrencies but the trustee pursuant to express trusts.

In contrast, in *B2C2 Ltd v Quoine*, the Singapore Court of Appeal (in a case concerning a breach of contract following an erroneous automated cryptocurrency trade) declined to provide a definitive view as to the status of cryptoassets as property.[15]

The *lex situs* or location of Bitcoin property for the purposes of determining the applicable law of the dispute was also considered by the E&W Courts in *Ion Science*. The court adopted academic analysis by Professor Andrew Dickinson in his book *Cryptocurrencies in*

Public and Private Law and held the *lex situs* of a cryptocurrency to be the place where the owner of it was domiciled, which in that case was England.

The clarifications on the status of cryptoassets as property and their *lex situs* brings some comfort to those seeking proprietary remedies and making crypto-related claims in the E&W Courts. However, given the novel features and variance that exists among cryptocurrencies, the question of whether a cryptocurrency amounts to property capable of being traced and enforced against will still need to be determined on a case-by-case basis.

The "*Where and When?*": Investigating the fraud and locating stolen cryptoassets

Cryptocurrencies generally exist within decentralised systems based on distributed ledger technology. Intermediaries are not required; often all that is needed to purchase cryptocurrency is internet access, a method of payment and a digital wallet. Upon acquiring cryptocurrency, the user is provided with a pair of cryptographic codes that are stored in their wallet: a public key (essentially an account number), which allows them to receive cryptocurrency at a pseudonymous address; and a private key (akin to a password), which enables the secure transfer of the cryptoasset to another wallet of their own or another user anywhere in the world using cryptographic authentication by a digital signature.

Each transaction is approved and verified by a consensus of participants on the network before it is logged as a unique entry on the relevant cryptocurrency's distributed digital ledger. The ledger constitutes a transparent and permanent chronological record designed to ensure that no cryptoasset is transferred to more than one user at any given time, and to prevent retroactive alteration of the record. The decentralised nature of the ledger means there is no central point of control; rather, the data is publicly stored and distributed on the network. Ledgers may be based on a variety of models depending on the cryptocurrency in question, but many of the best-known cryptocurrencies such as Bitcoin and Ethereum rely on blockchain technology, which sequentially records and links together blocks of transactions.

While these features of cryptocurrencies provide a level of anonymity, they also facilitate tracing of cryptocurrencies and the identities of those who own or control them.

Most instances of cryptocurrency fraud will involve the transfer of stolen or converted cryptocurrency to another or multiple cryptocurrency wallets. The private key to these wallets may be held by a third party where an exchange or custodian service has been used (generally in "hot" wallets connected to the internet), or by the wallet holder directly (either in "cold" wallets stored offline, or hot wallets).

Where the claimant's wallet address is known, transaction history can be located to trace the addresses to which transfers were made from the wallet, which may require examination of multiple layers of transactions before determining the ultimate destination of the stolen cryptoassets. The ease of identifying the wallets into which stolen cryptocurrency has been received may depend on where the wallet is stored and whether an exchange or custodian has access to it and/or possesses Know Your Client information to enable the identification of the wallet holder. Details shared by the user online may leave a helpful trail of usernames and email addresses that may aid their identification.

That said, there are some circumstances in which forensic tracing may not be possible; for example, where software or applications have been used to mix a cryptocurrency with different cryptocurrencies of the same value to conceal the original source of the cryptocurrency and obstruct the ability to trace through the blockchain. The forensic tracing of stolen cryptoassets can be conducted by engaging a specialist cryptocurrency investigation firm to forensically trace and provide the relevant answers to questions of "where and when?".

The "*Who?*": Identifying perpetrators of fraud and recipients of the proceeds

Forensic tracing exercises will assist in determining when and where fraudulently obtained cryptoassets have been transferred and/or subsequently converted to other cryptocurrencies or "fiat" currencies (government-issued currency such as US dollars). However, identifying the fraudsters and those who now hold or control the assets and preserving those assets pending any enforcement action will be key to any recovery of the assets. A claimant will therefore likely need to employ a multifaceted and speedy strategy to aid a successful recovery. Such strategy will likely require a combination of the following court orders available from the E&W Courts:

1. *Disclosure orders* to reveal: (a) the perpetrators of the fraud and any recipients of the stolen cryptoassets, and against whom causes of action to recover the stolen cryptoassets might exist; and/or (b) the location of the stolen cryptoassets (or their equivalent conversions). Such orders using the Bankers Trust and/or Norwich Pharmacal jurisdiction may be sought against persons responsible for the fraud (e.g. by way of ancillary disclosure orders in freezing/proprietary injunctions) and/or against third parties holding information about those persons, such as cryptocurrency exchanges or banks.
2. *Delivery up and/or search and seizure orders* to obtain possession of relevant documents or electronic information. Such orders are likely to merit consideration only in crypto fraud cases where relevant individuals or entities are known, as they necessarily involve the identification of the premises to be searched in the case of a search order and data/devices to be delivered up or imaged under a delivery up/imaging order. For example, where it is suspected that the defendant holds cryptocurrency in a cold wallet stored on an electronic device, an order to search the defendant's premises or an order requiring delivery up by the defendant of the wallet and any relevant keys or passwords might be sought. The primary purpose of such orders is preservation and preventing the destruction or alteration of material or information. However, delivery up orders can also be used to discover further information about where materials might be by requiring the respondent to provide, by way of affidavit, further information as to the whereabouts of relevant materials and who has them. Such orders therefore present a useful further tool that may be considered by a victim of crypto fraud, though are likely only to be practicable in cases of significant fraud given the costs involved including the fees of the supervising solicitor (a court requirement for a search order) in obtaining and executing such orders.
3. *Freezing and/or proprietary orders* to preserve any stolen cryptoassets or proceeds thereof pending any enforcement action. Such orders are often coupled with ancillary disclosure orders requiring the respondent to provide further information on oath regarding the whereabouts of assets.
4. *Related orders* to ensure that orders are validly served such as service by WhatsApp or use of encrypted online data rooms and/or orders for service out of the jurisdiction.

A number of the above have been employed with success in recent E&W Court cases:

1. *AA v Persons Unknown* concerned a cyberattack whereby the hacker installed malware and demanded payment in Bitcoin to enable the company to re-access its systems. The company's insurer (AA) paid the ransom of USD 950,000 via transfer of 109.25 Bitcoin. Having subsequently identified (through forensic tracing carried out by a crypto investigation firm) that 96 Bitcoin were transferred to wallets held with crypto exchange Bitfinex, AA brought applications before the E&W Courts seeking: (a) a Bankers Trust order ("**BTO**") and/or Norwich Pharmacal order ("**NPO**") against two crypto exchanges; (b) freezing and proprietary injunctions in respect of the Bitcoin and

accounts held with the crypto exchanges; and (c) consequential orders for service out of the jurisdiction and by alternative means. In the event, only the proprietary injunction was successfully obtained (see point (a) below as to why).

2. In *Ion Science*, the claimants had transferred 64.53 Bitcoin to a Swiss entity in the belief that they were investing in ICOs for genuine cryptocurrencies. However, the claimants never received any profits. The claimants brought successful applications for a proprietary injunction, worldwide freezing order ("**WFO**") and ancillary disclosure order against persons unknown and a disclosure order pursuant to the Bankers Trust jurisdiction and/or CPR 25.1(1)(g) against two further respondents who operated the cryptocurrency exchanges Binance and Kraken.
3. The claimant in *Fetch.ai* held cryptocurrencies in various accounts with the crypto exchange Binance. Those accounts were accessed by persons unknown who then traded with the cryptocurrencies and sold them at significant undervalue, effectively diminishing the value of the claimant's account and moving the claimant's cryptocurrencies to other accounts. The claimant brought successful applications for a proprietary injunction, WFO and ancillary disclosure against persons unknown and disclosure orders under the Bankers Trust/Norwich Pharmacal jurisdiction and/or CPR 25.1(1)(g) against the crypto exchange respondents.

There were several issues arising in the above cases that merit further discussion below and which signal that specific issues may need to be tested again in the E&W Courts to resolve persisting uncertainty.

The persons unknown jurisdiction

In most cryptocurrency fraud, the fraudsters and/or recipients of fraudulently obtained assets will not be identifiable by a prospective claimant even where the wallet known to hold the cryptocurrencies has been identified. Fortunately, the inability to name persons involved in the fraud or recipients of the proceeds at the outset is not necessarily a bar to any recovery action by the claimant in light of the developing "*persons unknown*" jurisdiction in English law.

The persons unknown jurisdiction enables claimants to seek injunctions and bring proceedings against defined categories of persons unknown and has been applied by the E&W Courts to various circumstances including: injunctions to restrain the publication of a stolen Harry Potter manuscript (*Bloomsbury Publishing Group v News Group Newspapers*);[16] an injunction restraining protests outside of a store on London's Regent Street (*Canada Goose v Persons Unknown*);[17] and a WFO against unknown persons responsible for an email fraud (*CMOC Sales & Marketing Limited v Persons Unknown*).[18] Recently, the persons unknown jurisdiction has been extended, as mentioned above, to the grant of a proprietary injunction in a cryptocurrency fraud case against unknown persons who fraudulently obtained Bitcoin in a cyberattack (*AA v Persons Unknown*).

Key considerations likely to be relevant when considering an application or proceedings against persons unknown in instances of cryptocurrency fraud include:

1. The need to identify specific *categories* of persons unknown and distinguish between them by reference to their alleged unlawful conduct, e.g. those who were involved in the fraud, those who received assets without having given proper consideration and those who are innocent recipients.[19] The E&W Courts have emphasised the need to maintain careful focus on what remedies are being sought against each of the categories of persons unknown, particularly where innocent recipients of fraudulently obtained cryptoassets are concerned.[20]
2. The requirement to make every effort to validly serve the claim and/or injunction on identifiable defendants and persons unknown. Permission should be sought for service

by alternative means such as email (e.g. where a hacker has identified themselves by email) or making the documents accessible on the internet or in a data room where relevant. Claimants will also need to consider the possibility that persons unknown may be outside of the jurisdiction and that an application for permission to serve out of the jurisdiction may be required.

3. Upon the subsequent identification of any individuals who were initially persons unknown, joining them to the proceedings as named defendants.

Issues in cryptocurrency fraud cases: Disclosure orders

Several English cases have recently considered applications for disclosure orders, under the Bankers Trust and Norwich Pharmacal jurisdiction and CPR 25.1(1)(g), against various crypto exchanges to obtain information about accounts/wallets and their ownership:

a. In *AA v Persons Unknown*, the court considered an application for BTO/NPO against two respondents who operated the Bitfinex exchange. Both respondents appeared to be located out of the jurisdiction and the court had to consider whether it had jurisdiction to require a company out of the jurisdiction to provide information pursuant to an E&W Court order and to serve that order out of the jurisdiction. Mr Justice Bryan referred to the decision in *AB Bank Limited, Off-shore Banking Unit v Abu Dhabi Commercial Bank PJSC*[21] ("***AB Bank***") where Mr Justice Teare had concluded that a NPO could not be obtained against an entity outside of the jurisdiction.[22] As a result and acknowledging the difficulties presented by *AB Bank*, the claimants instead invited Mr Justice Bryan to adjourn those applications and ultimately decided only to pursue the proprietary injunction, which was granted.
b. In *Ion Science*, the claimant sought a BTO and/or disclosure order pursuant to CPR 25.1(1)(g) against two respondents who operated the cryptocurrency exchanges Binance and Kraken. The issue presented by *AB Bank* arose again as both crypto exchange respondents were located out of the jurisdiction. Mr Justice Butcher distinguished the *AB Bank* decision on the basis that it related only to Norwich Pharmacal relief and did not concern a BTO and referred to *MacKinnon v Donaldson, Lufkin and Jenrette Securities Corporation*[23] where it was suggested that a BTO might be granted for service out of the jurisdiction in exceptional circumstances. Mr Justice Butcher considered the case before him to fall within exceptional circumstances as a case of "hot pursuit" and granted the BTO.
c. The same *AB Bank* issue arose in *Fetch.ai* where the Judge noted the existence of conflicting authorities on the point, but ultimately decided to adopt the approach taken in *Ion Science* and granted the BTO against the Cayman Islands-based crypto exchange. However, the Judge declined to make a NPO following *AB Bank.*

These decisions demonstrate some judicial willingness to extend the Bankers Trust jurisdiction to orders against crypto exchanges outside of the jurisdiction to assist in the recovery of stolen cryptoassets.

Issues in cryptocurrency fraud cases: Freezing orders and proprietary injunctions

Following clarification that cryptoassets are, in principle, to be considered property under English law, as referred to above, several decisions have granted freezing and/or proprietary injunctions in respect of accounts/wallets held with crypto exchanges and of the cryptoassets themselves. Various of those decisions have also highlighted important considerations for a claimant seeking such asset preservation injunctions in cases of crypto fraud:

1. *Blockchain Optimization S.A. & Anor v LFE Market Ltd & Ors*[24] is a reminder that applicants must be full and frank when applying for a WFO. In this case, a WFO was

granted in connection with investments made in a sham cryptocurrency token. The defendants applied to discharge the WFO for material non-disclosure. Specifically, it was alleged that the claimants' lawyers had failed to disclose that they had also acted in relation to the cryptocurrency token project, the relevance being that the lawyers may have had information relevant to whether the cryptocurrency token was a sham. The Judge considered the non-disclosure to be a material one (which can mean discharge of the WFO). However, the Judge ultimately continued the WFO on the basis that it was an innocent non-disclosure and the fact that another law firm's work on the project had been disclosed.

2. In *Fetch.ai*, the Judge voiced concern that the WFO sought against persons unknown might put an innocent recipient in inadvertent breach of the WFO with the risk of being in contempt of court. As a result, the injunction included a qualification to restrict the scope of the proprietary relief available in respect of innocent recipients to only those assets that such recipients either knew, or ought reasonably to have known, belong to the claimant or did not belong to the recipient.[25]

Issues in cryptocurrency fraud cases: Orders relating to service

Recent crypto fraud cases that have considered issues relating to service include:

1. *AA v Persons Unknown*: The court granted an order for service of the claim form by alternative means on persons unknown, which included permission to serve the claim form: (a) at any email address provided by the crypto exchange in respect of the relevant account; (b) by delivering or leaving it at any physical address provided by the crypto exchange in respect of the relevant account; and (c) by filing the claim form at court. As in *Ion Science*, the court also granted an order for service by alternative means in relation to the crypto exchange respondents on the basis that there was good reason and/or exceptional circumstances (including the urgency and the proprietary nature of the claim).
2. *Fetch.ai*: In relation to service on persons out of the jurisdiction, the court applied *Ion Science* and held that service could be effected based on jurisdictional gateways relating to the *lex situs* of the relevant cryptocurrency being England as the place of domicile of the owner of the cryptocurrencies that were the subject of the fraud.[26] The court held that an order for alternative service on an entity should be granted only where exceptional circumstances merited departure from the ordinary rules of service applicable, e.g. to ensure that the orders could be quickly drawn to the attention of the respondent concerned.[27]

In conclusion, as the Master of the Rolls stated: "*The justice system cannot stand on the side-lines, while every other aspect of our population's lives is transformed by technology.*" We will therefore increasingly see the E&W Courts responding as needed to ensure that fraudsters can be pursued across boundaries virtual and geographical with online court systems and the use of algorithms to manage and resolve disputes.

* * *

Endnotes

1. https://www.fca.org.uk/consumers/cryptoassets.
2. The Money Laundering and Terrorist Financing (Amendment) Regulations 2019.
3. The UKJT was one of six taskforces formed by the LawTech Delivery Panel, a team of industry experts and leading figures from government and the judiciary set up in 2018 to accelerate the digital transformation of the legal sector.

4. Legal Statement on Cryptoassets and Smart Contracts, UKJT 11 November 2019: https://35z8e83m1ih83drye280o9d1-wpengine.netdna-ssl.com/wp-content/uploads/2019/11/6.6056_JO_Cryptocurrencies_Statement_FINAL_WEB_111119-1.pdf, page 4.
5. https://www.judiciary.uk/wp-content/uploads/2021/03/20210309-MR-speech-ISDAs-Virtual-Annual-Legal-Forum-10-3-21-1.pdf, page 5.
6. Legal Statement: https://35z8e83m1ih83drye280o9d1-wpengine.netdna-ssl.com/wp-content/uploads/2019/11/6.6056_JO_Cryptocurrencies_Statement_FINAL_WEB_111119-1.pdf.
7. The Law Commission is currently considering whether digital assets could be capable of being possessed, notwithstanding that the concept of possession is presently limited to physical things. This conclusion of the UKJT together with the willingness of the E&W Courts to treat cryptoassets as property indicates that the concept that personal property must be either a thing in possession or a thing in action is now outdated.
8. *AA v Persons Unknown* [2019] EWHC 3556 (Comm), para. 61.
9. *AA v Persons Unknown* [2019] EWHC 3556 (Comm); *Ion Science Ltd v Persons Unknown and others* (unreported), 21 December 2020 (Commercial Court); and *Fetch.ai Limited & Anor v Persons Unknown & Ors* [2021] EWHC 2254 (Comm).
10. Digital Dispute Resolution Rules, UKJT, April 2021: https://35z8e83m1ih83drye280o9d1-wpengine.netdna-ssl.com/wp-content/uploads/2021/04/Lawtech_DDRR_Final.pdf.
11. *Vorotyntseva v Money-4 Limited* [2018] EWHC 2596 (Ch); *Robertson v Persons Unknown* (unreported), 15 July 2019.
12. *AA v Persons Unknown* [2019] EWHC 3556 (Comm); *Ion Science Ltd v Persons Unknown and others* (unreported), 21 December 2020 (Commercial Court); and *Fetch.ai Limited & Anor v Persons Unknown & Ors* [2021] EWHC 2254 (Comm).
13. [2020] NZHC 782.
14. [1965] AC 1175 (HL) at [1247]–[1248].
15. *B2C2 Ltd v Quoine Pte Ltd* [2020] SGCA(I) 02.
16. [2003] EWHC 1205 (Ch).
17. [2020] EWCA Civ 303 at [82].
18. [2017] EWHC 3599 (Comm).
19. *Fetch.ai* at [5]–[7].
20. *Ibid.*
21. [2016] EWHC 2082 (Comm).
22. *AA v Persons Unknown* at [46].
23. [1986] Ch 482.
24. [2020] EWHC 2027 (Comm).
25. *Fetch.ai* at [7].
26. *Fetch.ai* at [14]–[23] and [45].
27. *Fetch.ai* at [46].

Jane Colston
Tel: +44 207 851 6059 / Email: jcolston@brownrudnick.com

Jane specialises in complex civil fraud, company and partnership and financial services disputes. She is ranked in *Who's Who Legal* (*WWL*) *2021* as "Global Elite Thought Leader" for Asset Recovery ("*impressed peers... consider her a superstar*") and "Thought Leader" in Litigation ("*a top-class lawyer who garners strong support thanks to her great expertise in high-value commercial banking, contract and tort disputes*"). Jane is also ranked in *Chambers*' "Litigation Support Global 2021" ("*Market peers and clients consider her to be… a formidable litigator*") and was *WWL 2020*'s Asset Recovery Lawyer of the Year.

Jane leads Brown Rudnick's Supervising Solicitors team (https://brownrudnick.com/practice/supervising-solicitors-search-orders/) and serves as its Diversity & Inclusion Partner (https://brownrudnick.com/about/diversity-equity-inclusion/).

Jessica Lee
Tel: +44 207 851 6140 / Email: jslee@brownrudnick.com

Jess is an Associate in Brown Rudnick's Litigation & Arbitration Practice Group. Jess has significant experience in complex and high-value commercial litigation with a particular focus on civil fraud and asset recovery claims and corporate and financial services disputes. She acts in numerous complex cross-border civil fraud cases and advises on freezing, proprietary, and disclosure injunctions. Jess is part of Brown Rudnick's Supervising Solicitors team (https://brownrudnick.com/practice/supervising-solicitors-search-orders/) and has recent experience in search and delivery up orders and their execution. Jess has also advised on significant investigations and compliance matters including investigations by the US DoJ and the Serious Fraud Office.

Imogen Winfield
Tel: +44 207 851 6078 / Email: iwinfield@brownrudnick.com

Imogen is an Associate in the International Disputes team in Brown Rudnick's London office. She has experience in a wide range of commercial disputes, including complex and high-value breach of contract and negligence claims involving financial institutions, as well as significant pre-action matters. Imogen has acted for senior executives in connection with regulatory investigations and has a particular interest in disputes arising out of financial contexts. Imogen also has experience of search orders and is part of Brown Rudnick's Supervising Solicitors team (https://brownrudnick.com/practice/supervising-solicitors-search-orders/).

Brown Rudnick LLP

8 Clifford Street, London W1S 2LQ, United Kingdom
Tel: +44 207 851 6000 / URL: www.brownrudnick.com

Australia

Peter Reeves, Robert O'Grady & Emily Shen
Gilbert + Tobin

Government attitude and definition

Australia has generally been regarded as a relatively friendly and stable jurisdiction for blockchain and cryptocurrency businesses to operate in. This has been driven in part by Australia's overall approach to the financial technology (**fintech**) sector, with the Commonwealth Government of Australia (**Government**) supportive of broad growth and innovation. There has been a proliferation of product offerings from the Australian blockchain and cryptocurrency community, and the Australian approach to the sector has broadly remained supportive of new and innovative financial services and products using or transacting cryptocurrencies. In part, the expansion of the sector in Australia has been led by businesses in the payments, crypto asset, lending, investment and custodial services spaces.

To date, the Government has taken a largely non-interventionist approach to the regulation of cryptocurrency, allowing the landscape to evolve at a faster rate without significant regulatory limitation. Such growth remains a priority for the Government, emphasised by its Select Committee on Australia as a Technology and Financial Centre publishing its third issues paper in March 2021, having amended its scope of matters to include opportunities and risks in the digital asset and cryptocurrency sector.

Currently, Australian law does not equate digital currency with fiat currency and does not treat cryptocurrency as "money". The Reserve Bank of Australia (**RBA**), Australia's central bank, indicates no immediate plans to issue a digital dollar akin to money (often referred to as an "eAUD"). Although the RBA has been involved in numerous projects to explore the potential use and implications of a wholesale central bank digital currency (**CBDC**), it maintains that there is currently no public policy case to issue a retail CBDC.

While the Government has not significantly intervened in cryptocurrencies and related activities, there has been general clarification of the application of Australian regulatory regimes to the sector. For example, since 2018, digital currencies have been caught by Australia's anti-money laundering and counter-terrorism financing (**AML/CTF**) regime. This amendment recognised the movement towards digital currencies becoming a popular method of paying for goods and services and transferring value in the Australian economy and addressed the possibility of digital currencies being used for money laundering and terrorism financing (**ML/TF**).

As well as in payments, there has been a growing expectation that crypto assets (including cryptocurrencies) will become accepted as an investment asset class. In June 2021, Australia's primary corporate, markets, consumer credit and financial services regulator, the Australian Securities and Investments Commission (**ASIC**), launched a consultation process on its proposals to clarify expectations for crypto assets that form part of the underlying assets of exchange-traded products (**ETPs**) and other investment products.

Cryptocurrency regulation

While there have been legislative amendments to accommodate the use of cryptocurrencies, these have predominantly focused on the transactional relationships (e.g., the issuing and exchanging process) and activities involving cryptocurrencies, rather than the cryptocurrencies themselves.

ASIC has reaffirmed 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 has been no legislation created to deal with cryptocurrencies as a discrete area of law, this does not hinder 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 coins (or tokens). This depends 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. This is discussed in more detail under "Sales regulation" below.
- There has also been a proliferation of lending activities in relation to cryptocurrency. To the extent these lending 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 the requirement to be licensed.

ASIC has recently launched a consultation process on its proposals to clarify expectations for crypto assets that form part of the underlying assets of ETPs and other investment products. ASIC proposes to set 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 the use of 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. The consultation also includes ASIC's proposed good practices in relation to how fund asset holders are required to custody crypto assets, as well as ensuring adequate risk management systems are in place. ASIC proposes to include crypto assets as a distinct asset class on AFSL authorisations for managed investment schemes, but expects that this will only authorise the holding of Bitcoin and Ether in the short term. The consultation process remains open at the time of writing and it is expected that industry feedback will inform how ASIC intends to apply the proposals in the future.

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*) (most recently updated in March 2021) 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 still be 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

Of particular concern to those dealing with cryptocurrencies is whether the relevant cryptocurrency constitutes a financial product triggering financial services licensing and disclosure requirements. Entities carrying on a financial services business in Australia must hold an AFSL or be exempt. The definitions of "financial product" or "financial service" under the Corporations Act are broad and ASIC has indicated in its information sheet, *INFO 225 Initial coin offerings* (**INFO 225**), that cryptocurrency with similar features to existing financial products or securities will trigger the relevant regulatory obligations.

In INFO 225, ASIC indicated that the legal status of cryptocurrency is dependent upon the structure of the ICO and the rights attaching to the coins or tokens. ASIC indicated that what is a right should be interpreted broadly. Depending on the circumstances, coins or tokens 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 the Australian financial services regulatory regime. In INFO 225, ASIC provided 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.

Broadly, entities offering coins or tokens that can be classified as financial products 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 cryptocurrencies may also be required to hold an AFSL and the operator of a cryptocurrency exchange may be required to hold an Australian market licence if the coins or tokens traded on the exchange constitute financial products.

Generally, ASIC's regulatory guidance is consistent with the position of regulators in other jurisdictions. ASIC has also recommended that companies wishing to conduct an initial coin offering (**ICO**) or other token sale seek professional advice, including legal advice, and contact its Innovation Hub (discussed in detail below, "Promotion and testing") for informal assistance. This reflects its willingness to build greater investor confidence around cryptocurrency as an asset class. However, ASIC has emphasised consumer protection

and compliance with the relevant laws and has taken action as a result to stop proposed token sales targeting retail investors due to issues with disclosure and promotional materials (the requirements of which are discussed below) as well as offerings of financial products without an AFSL.

In 2019, the Treasury consulted on ICOs and the relevant regulatory frameworks in Australia; however, no outcomes of this consultation have been reported to date.

Marketing

ASIC's recognition that a token sale may involve an offer of financial products has clear implications for the marketing of the token sale. For example, an offer of a financial product to a retail client (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 the provider's fee structure, to assist a client in deciding whether to acquire the cryptocurrency from the provider. In some instances, the marketing activity itself may cause the token sale to be an offer of a regulated financial product.

Under the Corporations Act, depending on the minimum amount of funds invested per investor and whether the investor is a "sophisticated investor" or wholesale client, an offer of financial products may not require regulated disclosure.

Cross-border issues

Carrying on a financial services business in Australia will require a foreign financial services provider (**FFSP**) to hold an AFSL, unless relief is granted. Entities, including FFSPs, should note that the Corporations Act may apply to an ICO or token sale regardless of whether it was created and offered from Australia or overseas. Currently, Australia has a foreign AFSL (**FAFSL**) regime for FFSPs regulated in certain jurisdictions that enables FFSPs regulated in those jurisdictions to provide financial services to wholesale clients (similar to the concept of an accredited investor under US law) in Australia without holding an AFSL. The FAFSL regime replaces the previous passporting arrangements Australia had in place (though FFSPs already relying on passport relief may do so until 31 March 2023). The Treasury is currently consulting on unwinding the repeal of passport relief and/or proposing new relief for FFSPs and is also consulting on a fast-track licensing regime for FFSPs seeking to apply for an AFSL. At the time of writing, no outcomes have been released in relation to either of these consultations.

Foreign companies taken to be carrying on a business in Australia, including by issuing cryptocurrency or operating a platform developed using ICO proceeds, 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.

Promoters should also be aware that if they wish to market their cryptocurrency to Australian residents, and the coins or tokens are considered a financial product under the Corporations Act, they will not be permitted to market the products unless the requisite licensing and disclosure requirements are met. Generally, a service provider from outside of Australia 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

From 5 October 2021, issuers and distributors of financial products must comply with design and distribution obligations (**DDO**), which may impact the way cryptocurrencies are structured and token sales are conducted in the future. Issuers and distributors must implement effective product governance arrangements, which include (among other things) a target market determination subject to review triggers. The DDO aim to ensure that financial products are targeted at the correct category of potential investors. Issuers and distributors are required to comply with the DDO from 5 October 2021.

Product intervention powers

ASIC also has temporary 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. These powers are highly likely to impact marketing and distribution practices in the cryptocurrency sector where cryptocurrencies fall within the remit of the powers.

Consumer law

Even if a token sale is not regulated under the Corporations Act, it may still be 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. As such, care must be taken in token sale promotional material to ensure that buyers are not misled or deceived and that the promotional material does not contain false information. In addition, promoters and sellers are prohibited from engaging in unconscionable conduct and must ensure that the coins or tokens issued 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 token sales (regardless of whether it involves a financial product). ASIC has indicated that misleading or deceptive conduct in relation to token 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 token sale or a crypto asset by engaging in (or arranging for others to engage in) certain trading strategies;
- failing to disclose appropriate information about the token sale; or
- suggesting that the token 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 token 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).

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 (that is, 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 views 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.

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 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 26% or 30%. However, if the issued coins are characterised as equity for tax purposes or are issued in respect of a borrowing of money, the ICO proceeds may not be assessable to the issuer.

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;
- 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 begin enforcing tax liabilities more aggressively.

Money transmission laws and anti-money laundering requirements

Since 2018, 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$111,000, 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 are also required to 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 June 2021, AUSTRAC promoted the Financial Action Task Force's (of which Australia is a member nation) red flags guidance for indicators of ML/TF, which sets out best practice for regulators and reporting entities and is expected to inform how AML/CTF legislation relating to digital currency is developed.

Promotion and testing

Regulators in Australia have generally been receptive to blockchain and cryptocurrency and have sought to improve their understanding of, and engagement with, businesses by regularly consulting with industry on proposed regulatory changes. As part of this mandate, 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 has engaged 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 (**GFIN**), which was formally launched in January 2019 by a group of financial regulators across 29 member organisations. The GFIN is dedicated to facilitating regulatory collaboration in a cross-border context and provides more efficient means for innovative businesses to interact with regulators.

AUSTRAC Innovation Hub

AUSTRAC's Fintel Alliance is a private-public partnership seeking to develop "smarter regulation". This includes setting up an Innovation Hub targeted at improving the relationship between new businesses operating in innovative spaces like cryptocurrency and blockchain, and the Government and regulators. While the hub has generally been targeted at fintech businesses more broadly, cryptocurrency and blockchain-related businesses can enter the hub's regulatory sandbox to test financial products and services without risking regulatory action or costs.

Ownership and licensing requirements

At the time of writing, there are currently no explicit restrictions on investment managers owning cryptocurrencies for investment purposes. However, investment managers may be subject to Australia's financial services regulatory 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 cryptocurrencies held that are financial products will be providing financial product advice under the Corporations

Act and must hold an AFSL or otherwise be exempt from the requirement to be licensed. 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 investment managers wish to custody cryptocurrencies that are financial products on behalf of clients.

Australia has also seen a rapidly rising interest in robo-advice or digital advice models. The provision of robo-advice is where algorithms and technology provide 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*. 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

More generally, 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 Corporate Plan 2020 to 2024, ASIC stated that a key priority was to improve management of key risks and that, partly as a result of the COVID-19 pandemic, entities "without appropriate systems in place are increasingly vulnerable to cyber attacks, data breaches, technology failures and system outages". CERT Australia (now part of the Australian Cyber Security Centre) noted that there has been an increase in cryptomining malware affecting businesses' resources and processing capacity.

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 651 Cyber resilience of firms in Australia's financial markets: 2018–19*, identifies key trends in cyber resilience practices and highlights existing good practices and areas for improvement. ASIC has previously provided two reports, namely *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.

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 cryptocurrency being captured by declaration obligations under the AML/CTF Act for the time being.

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.

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, the AML/CTF Rules outline 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 generally are 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.

In April 2016, the Report on the Statutory Review of the Anti-Money Laundering and Counter-Terrorism Financing Act 2006 and Associated Rules and Regulations (**AML/CTF Report**), which contained 84 recommendations to improve Australia's AML/CTF regime, was released. The AML/CTF Report contemplated two phases of consultation and implementation, with Phase 1 including priority projects completed in 2017, while Phase 2 progresses major, long-term reforms. These reforms should, among other things, clarify record-keeping requirements and reporting obligations for reporting entities.

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 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 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 is a partner in Gilbert + Tobin's Corporate Advisory group and leads the Fintech practice at G + T. 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.

Robert O'Grady
Tel: +61 2 9263 4241 / Email: raogrady@gtlaw.com.au

Robert is a lawyer in G + T's Corporate Advisory 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 is a lawyer in G + T's Corporate Advisory group with a focus on fintech, financial services regulation and funds management. She has been involved in advising a range of clients across the financial services, fintech and digital sectors on issues relating to financial services regulation, payments, digital platforms, crypto and other tokenisation deployments, credit and BNPL, funds establishment and structuring, AML/CTF and blockchain solutions.

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.

Despite the COVID-19 pandemic, 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 over the last two 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 or DeFi applications and non-fungible tokens.

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 registration of virtual asset service providers.

While national initiatives in this field are welcome, we expect that the issuance of, and services around, cryptoassets will in the mid-term be regulated on a European level, with the European Commission having published draft legislation on a markets in cryptoasset regulation applicable to cryptoassets not covered by existing EU financial services legislation (e.g. MiFID II, the E-Money Directive, PSD II).

Cryptocurrency regulation

In Austria, cryptocurrencies initially caused quite a headache for financial market regulators, in particular as no statutory definition of cryptocurrencies existed. Meanwhile different definitions emerged that are used in the crypto space, such as "virtual currency", "cryptocurrency", "cryptoasset", "coin" or "token". However, currently there is only one legal definition for the term "virtual currency", which was introduced by the 5th Money Laundering Directive (see Article 3 (18) (EU) 2018/843). According to this, virtual currencies are 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".

In addition to this, there are no cryptocurrencies or fintech-specific laws or regulations that have currently been enacted. Irrespective of the foregoing, according to the Austrian regulator, the FMA, cryptocurrencies are typically characterised as follows:

- they are not issued by any central bank or governmental authority;
- new units of value are typically created using a predefined procedure within a computer network (commonly referred to as "mining");
- there is no central authority that verifies or manages transactions;
- transactions are recorded on a decentralised, publicly held ledger (commonly referred to as "blockchain") and, once executed, cannot be revoked;
- electronic wallets may be used to store and manage virtual currencies (commonly referred to as "wallets"); and
- decentralised network – Peer-to-Peer network.

Furthermore, cryptocurrency is currently not treated as "money" or otherwise given equal status with domestic or foreign fiat currency in Austria. Likewise, there are not yet any cryptocurrencies that are backed by the Austrian government or the Austrian National Bank.

From an Austrian financial services regulatory perspective, cryptocurrencies are currently neither treated as financial instruments (in particular, as securities or derivatives) nor as currency (domestic or foreign), but as commodities. It is worth noting, however, that derivative instruments referencing cryptocurrencies or tokens will qualify as financial instruments under the second Markets in Financial Instruments Directive ("MiFID II") and hence will be covered by financial services regulation under MiFID II and the Markets in Financial Instruments Regulation.

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. Depending on their precise features/content, the operation of various business models based on cryptocurrencies may trigger licensing requirements under the Austrian Banking Act (*Bankwesengesetz*; "BWG"), the Austrian Alternative Investment Fund Managers Act (*Alternative Investmentfonds Manager-Gesetz*; "AIFMG") or the Austrian Payment Services Act (*Zahlungsdienstegesetz*; "ZaDiG"), and/or prospectus requirements under the EU Prospectus Regulation or the Austrian Capital Markets Act (*Kapitalmarktgesetz*).

In this respect, the general legal framework also applies to cryptocurrencies and new technologies. The FMA is known to apply a "technology-neutral" supervisory approach, meaning that products and services are subject to the same regulatory framework as "traditional" products/services. The underlying rationale is "same risk – same rules". If and to what extent financial services regulation applies primarily depends on the actual product features/activities.

Innovative business models involving cryptocurrencies may be subject to licensing requirements and governed by:

- the BWG – for example, if funds are raised for investment into cryptocurrencies;
- the 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 AIFMG – for example, if funds are raised for investment into cryptocurrencies according to a pre-defined investment strategy; and
- the Electronic Money Act – when issuing electronic money.

The FMA has published further guidance on the regulatory treatment of certain activities around cryptocurrencies, ICOs/ITOs and fintech in the fintech navigator section of its website at https://www.fma.gv.at/en/cross-sectoral-topics/fintech/fintech-navigator/.

Key areas to note are the following:

- Purely technical services do not require a licence under financial services regulation. If, however, a technical billing service also includes transfer of funds, this would no longer be considered a purely technical service and would need to be tested against licensing requirements under the BWG, the AIFMG and the Austrian Electronic Money Act.
- Alternative currencies, payment instruments or 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 (there is a licensing exception for restricted networks, but this has become increasingly strict following the implementation of Directive 2015/2366/EU ("PSD II")). Also, if accounts are operated in connection with currencies, payment instruments or means of payment through which payments are made, the entity holding the accounts may be obliged to become licensed as a payment service provider.
- If capital is raised in order to invest proceeds into cryptocurrencies or mining, this could be regulated as a banking business (deposits business) or as managing an alternative investment fund ("AIF") under the AIFMG if funds are invested in accordance with a defined investment strategy and returns in each case depend on the performance of the underlying investment. If the capital-raising is structured through the issuance of shares or similar participation in a corporation or partnership, this may also trigger prospectus requirements under Austrian securities laws (see "Sales regulation", below).
- Online platforms for acquiring virtual currencies that also settle/process payments in domestic or foreign currency through their own accounts may require a licence under the AIFMG. Generally, if funds pass through the provider's accounts, this will trigger a licence requirement under payment services regulations. Some online service providers therefore cooperate with licensed partners and transfer funds via their accounts.
- Brokers of new or alternative payment methods may need to become licensed if they are considering intermediating deposits or loans/insurance. This would be the case if an app or online platform was linked to a specific deposit/current account. The mere listing of product information, for example, via product comparison portals, would not require a licence.
- While merely buying and selling virtual currencies in one's own name and for one's own account generally does not trigger a licence requirement, the buying and selling of virtual currencies may form part of business models that do require a licence. For instance, the operation of a Bitcoin vending machine may trigger a licence requirement, depending on its features. Also, clearing a Bitcoin vending machine and subsequently transferring any funds collected to a third party may require a payment services licence for money remittance under the AIFMG.
- There is currently no deposit guarantee scheme and no legal investor protection scheme for cryptocurrencies or tokens.

Given the diversity, complexity and rapid evolution of business models in the fintech space, the regulatory treatment of any business models involving cryptocurrencies or tokens will need to be assessed on a case-by-case basis.

The FMA therefore encourages discussion of the regulatory treatment prior to engaging in any business activity. It has set up a dedicated specialist team and fintech contact portal dedicated to those areas, which handles all fintech-related queries.

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 a token's terms and conditions/features, certain token offerings/sales may be subject to prospectus requirements under Austrian securities laws unless a prospectus exemption applies. Each offering must be assessed on a case-by-case basis and the regulatory assessment will depend on the specific technical, functional and economic design of the instruments offered.

For 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:

- 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 prospectus requirements under the EU Prospectus Regulation unless a prospectus exemption applies.
- Utility tokens: There are many designs of 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. No prospectus will need to be published if a prospectus exemption applies. This will be the case if the respective tokens are only offered to qualified investors, or if the offering is directed to fewer than 150 persons who are not qualified investors per EEA Member State, or if the minimum investment is at least €100,000 per investor.

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.

Taxation

Income tax treatment of cryptocurrencies

In general, capital gains from the sale of cryptocurrencies held as business assets, and income from commercial activities related to cryptocurrencies (e.g. mining, brokerage), are subject to progressive income tax rates of up to 55% for individuals and 25% for corporations.

Special rules apply to cryptocurrencies treated as investment assets and other (non-business) assets:

- Cryptocurrencies are treated as investment assets in case the taxpayer uses them to generate interest income. In this case, capital gains from a subsequent sale are taxed at 27.5% for individuals (taxation at lower progressive income tax rates optional) or at 25% for corporations.
- In case cryptocurrencies are not used to generate interest income, are only acquired and sold occasionally (private sales) and are not part of a business (non-business assets), capital gains are subject to taxation of up to 55% for individuals only if they are acquired and sold within 12 months. A tax exemption applies if capital gains do not exceed €440 per calendar year. In case cryptocurrencies are held for longer than 12 months, capital gains are not taxable.

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 the accounts may be obliged to become licensed as a payment service provider.

Activities involving cryptocurrencies are subject to AML requirements (including know-your-customer checks and AML prevention systems) if they:

- require a licence under financial services regulation (e.g. as provision of payment services); and
- 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.

With the entry into force of the Financial Markets Anti-Money Laundering Act ("FM-GwG"), which implements the 5th Money Laundering Directive, the FMA has become the competent authority for registrations and ongoing supervision of service providers relating to virtual currencies (as defined in Article 2 No 21 FM-GwG) regarding the prevention of money laundering and terrorist financing.

Service providers that intend to provide one of the following services in relation to virtual currencies in or from Austria are required to register with the FMA before the start of the services:

- services to safeguard private cryptographic keys, to hold, store and transfer virtual currencies on behalf of a customer (custodian wallet providers);
- exchanging of virtual currencies into fiat currencies and *vice versa*;
- exchanging of one or more virtual currencies between one another;
- transferring of virtual currencies; and
- the provision of financial services for the issuance and selling of virtual currencies.

Promotion and testing

True to the government's motto "advice instead of punishment", the Austrian Ministry of Finance has finally 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 a 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 Fintech and 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 is 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 from currently more than 15 countries (http://thinkblocktank.org/). Ursula 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 is 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 from currently more than 15 countries (http://thinkblocktank.org/) 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 / Fax: +43 1 534 37 66100 / URL: www.schoenherr.eu

Brazil

Flavio Augusto Picchi & Luiz Felipe Maia
FYMSA Advogados

Government attitude and definition

The Real 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 alternative payment methods, they are classified as goods or movable property. Cryptoassets were first defined in May 2019, when the Federal Revenue Office (*Secretaria Especial da Receita Federal do Brasil* – "**RFB**") issued a normative ruling (*Instrução Normativa*) to introduce reporting requirements for transactions involving such assets.[1]

According to RFB Normative Ruling No. 1,888/19, 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 that is not recognized as a currency*".[2] It also defines crypto exchanges as "*legal entities, either engaged in financial activities or not, offering services with respect to cryptoasset transactions, including brokerage, negotiation or custody, and which may accept any means of payment, including other cryptoassets*".

Earlier in 2013, Brazil adopted Law No. 12,865/13 to regulate the adoption of "electronic currencies", which are distinguished from virtual currencies.[3] In 2014, the Brazilian Central Bank (*Banco Central do Brasil* – "**BCB**") clarified in its Policy Statement No. 25,306 that virtual currencies are neither issued nor guaranteed by any monetary authority and are not guaranteed to convert to any sovereign currency.[4] Later, in 2017, Policy Statement No. 31,379 ratified its understanding and warned that companies engaged in selling and storing cryptocurrencies on behalf of their users are not regulated or supervised by national authorities.[5]

Even though they are not considered money and there are no specific regulations on the matter, government attitude towards cryptoassets is increasingly positive. Regulators are reviewing promising technologies for societal impact and transformation, notably in the financial sector, but not limited to it. Federal, state, and local authorities are engaged in efforts to develop ecosystems to make use of blockchain and cryptoassets as channels for innovation in the public and private sectors.

In March 2018, Decree No. 9,319/18 introduced the framework to approach digital transformation policies with the Brazilian Digital Transformation Strategy.[6] It was followed by Decree No. 10,332/20 in April 2020, which adopted the Federal Digital Government Strategy, aiming to embrace the potential for betterment of digital public administration services.[7]

In March 2021, Law No. 14,129/21 officially launched the Digital Government Program, setting rules and principles aiming to enhance efficiency in public services, reduce

bureaucracy, foster innovation, and enable digital transformation throughout government bodies.[8] The Special Secretariat for State Modernization (*Secretaria Especial de Modernização do Estado* – "**SEME**") has been developing with public entities the Brazilian blockchain network. SEME established a technical group to address possible uses of the technology to increase the efficiency of public sector entities.[9]

The Federal Court of Accounts (*Tribunal de Contas da União*) published in August 2020 a summary report about the topic, highlighting the advantages of adopting blockchain and distributed ledger technologies in the public administration.[10]

The National Monetary Council (*Conselho Monetário Internacional* – "**CMN**") is the major institution of the Brazilian financial system, and supervises the activities of other regulatory and enforcement agencies.[11] Under this institutional framework, BCB performs its functions as monetary, regulatory and supervisory authority in accordance with guidelines issued by CMN.[12] On its turn, the Securities and Exchange Commission (*Comissão de Valores Mobiliários* – "**CVM**") is in charge of commodities and securities markets.[13] Finally, the Superintendence of Private Insurances (*Superintendência de Seguros Privados* – "**SUSEP**") is responsible for the supervision and control of the insurance, open private pension funds and capitalisation markets.[14]

In June 2019, those main four agencies under the Ministry of Economy (RFB, BCB, CVM, and SUSEP) agreed to introduce sandbox programmes to implement emerging technologies under more relaxed regulatory provisions. The agencies announced they would also be integrating blockchain applications to their workflow.[15] A noteworthy move came in August 2020 upon adoption of the Platform for Regulatory Entities' Data Integration (*Plataforma de Integração de Informações das Entidades Reguladoras*), an initiative to streamline licences through blockchain technology, by instantly sharing their databases.[16]

An example is the bConnect network, which since mid-2020 integrates the Mercosur countries' customs agencies to expedite the exchange of information about exporters through use of smart contracts.[17] As a consequence, different means of local certifications are integrated regardless of their underlying technologies. In November 2020, Decree No. 10,550/20 specifically allowed blockchain applications to be used in foreign trade.[18]

Maybe the boldest initiative is the adoption of a Central Bank Digital Currency ("**CBDC**") by BCB. It released the general guidelines for a Brazilian CBDC in May 2021, after initial assessments and discussions by a working group created in August 2020,[19] aiming to discuss and evaluate the potential benefits and impacts of the Brazilian Real in a digital format.[20] The "Real Digital" could support BCB's strategic objective of fostering financial citizenship and strengthen the relationship with society and public powers. An electronic currency can increase the safety of handling and custody of cash, in addition to creating monetary policy instruments.

While not defined as a state-backed digital currency, a promising project is under development by the Brazilian National Development Bank (*Banco Nacional de Desenvolvimento Econômico e Social* – "**BNDES**").[21] BNDESToken could be classified as a stablecoin, i.e., a digital and tokenised version of the Real issued by BNDES in some financing transactions. In proof-of-concept tests, the prototype solution was implemented using smart contracts from the Ethereum network. The technology was deemed feasible and the project aims to enhance transparency in the lending process and credit performance, with potential applications in combatting corruption.[22]

Cryptocurrency regulation

Technological transformations bring about significant challenges to the Brazilian legal system. The digital asset regulatory framework currently comprises ordinances by administrative authorities, but no specific laws have been enacted to govern the matter. Despite the legislative gap, a series of recent initiatives by Brazilian legislators are under analysis by the Brazilian Congress and discussions are still under way. Most of the bills of law aim to address societal concerns and decrease systemic vulnerabilities regarding fraud and Ponzi schemes. Some of them introduce probate and succession rules for digital assets, as discussed in more detail below.

At the House of Representatives, the most significant bills regarding cryptoassets were recently merged so that a unified legal framework could be drawn. Bill of Law No. 2,303/15 was the first attempt to regulate cryptoassets. It was drafted and further discussed to address concerns with fraudulent schemes and increase money laundering prevention;[23] however, it relied on a questionable generalisation of cryptocurrencies as a sort of "electronic currency" and embraced, under the same rules, 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 AML legislation.

This statutory proposal was recently restated with further provisions, and presented as Bill of Law No. 2,060/19, which brings forth more complete and precise definitions regarding cryptographic values, instruments, assets, tokens, rights and services, and virtual tokens. It also introduced rules for issuance of cryptoassets and defines as a criminal offence their fraudulent use in "pyramid" or Ponzi schemes and irregular transactions with cryptoassets.[24]

Additionally, at the Senate there are a number of bills addressing 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 are focused on fighting against money laundering and other illicit practices. For instance, Bill of Law No. 4,207/20 draws on rules regarding "*the issuance, intermediation, custody, distribution, clearing, and administration of cryptoassets*", classifying such uncompliant transactions as crimes against the national financial system, i.e., white-collar felonies.

In line with concerns about financial prudential regulation, Bills of Law Nos 3,825/19 and 3,949/19 were presented to set forth the legal framework of crypto exchanges and similar platforms, by adoption of compliance procedures and operational licences to be assigned by BCB (except in especially defined exemption cases). Bill of Law No. 3,825/19 also criminalises the unauthorised brokerage of such exchanges and platforms as crime against the national financial system and subject to civil, administrative, and criminal provisions addressed in consumer protection laws.

Sales regulation

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, as amended.[28] In October 2017, CVM addressed its initial concerns about initial coin offerings ("**ICOs**"). According to CVM, "*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*".[29]

Shortly thereafter, CVM was faced with its first case involving an 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; those were not deemed as 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.[30] While stressing that not all ICOs are public offers of securities, CVM stressed that non-compliant offers would be considered illicit and, as such, subject to applicable sanctions and penalties under the securities laws framework.

That was the case in October 2019, when CVM brought its first enforcement investigation.[31] Promoters of a cryptocurrency were accused of conducting an unregistered ICO, and the commission found that several provisions of securities regulations were violated. CVM commissioners unanimously agreed in October 2020 with the rapporteur's function-over-form analysis in his opinion, according to which the classic definition of security was met. The offer was identified as aiming 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 against the promoters a disgorgement fine in excess of BRL 775,000.[32] The case is now under administrative appeal.

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.[33] In several cases, Ponzi schemes have been identified, leading to several criminal indictments by public prosecutors.

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. A popular football team from Rio de Janeiro, Vasco da Gama, has initiated a tokenisation project "Futecoin", a joint venture with the leading Brazilian crypto exchange Mercado Bitcoin, and received a no-action letter from CVM after a request for guidance. FIFA, the international governing body of football, issued rules for transfer of players, including the "solidarity mechanism", which allows a club that previously supported an athlete's training and education to obtain a fraction of future revenues earned by the athlete. Futecoins are virtual tokens backed by expected revenues from such economic rights with regard to players mentored by Vasco da Gama. The project allows fans to financially support the club, engage in its marketing efforts, and diversify their own investments. Cruzeiro, another major Brazilian football club, is also engaged in a similar project.

Taxation

Brazilian tax laws do not provide for specific provisions regarding cryptocurrencies. Given that these assets 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 case gains are limited to BRL 30,000 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). 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 Brazilian Congress to include preventive reporting obligations. Since no specific statute addresses money laundering activities with respect to cryptocurrencies, general provisions apply to the crypto industry.

Law No. 9,613/98 is the Brazilian Anti-Money Laundering Law, as amended by Law No. 13,974/20, and created the Council of Financial Activities Control (*Conselho de Controle de Atividades Financeiras* – "**COAF**").[34] This federal agency is at the centre of financial intelligence and in charge of suspected cases of concealment of assets and values, money laundering and terrorism financing.[35] 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 markets, insurance, and pension fund players are the most common entities subject to its supervisory activities, companies in charge of accounting, jewellery and precious metals, factoring, lotteries, and art dealing must report suspect 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 recently restated in March 2021 by COAF Resolution No. 36/21.[36] 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.[37]

RFB Normative Ruling No. 1,888/19 requires cryptocurrency exchanges to report their transactions to COAF, but 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 of 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.[38]

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 legacy banks to close exchange accounts.

In January 2020, BCB Circular No. 3.978/20 imposed policy, procedures, and internal controls to be adopted by regulated entities to prevent the use of the financial system for such illegal activities.[39] It was followed by BCB Circular No. 4.001/20, which presents 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 recently amended in July 2021 to include additional measures and mandatory information to be followed by financial institutions.[40]

Promotion and testing

As a result of the conversion of Provisional Measure (a type of Decree-Law issued by the President) No. 889/19 in April 2019, Federal Law No. 13,874/19 – the "**Economic Freedom Law**" – was enacted in September 2019 to establish the Declaration of Economic Freedom Rights.[41] It purported to simplify governmental requirements and reduce bureaucracy for economic players, as well as to promote cultural changes in interactions among private businesses and Brazilian authorities. It set forth provisions to assure minimum state intervention and reduction of government control of the markets, as well as expand initiatives such as regulatory sandboxes to foster competition and innovation in the Brazilian economy.

The above-referenced joint statement by BCB, CVM, SUSEP and RFB in June 2019 towards adoption of sandboxes was a direct reflex of the Provisional Measure and the following approved Economic Freedom Law. As a direct consequence, in October 2020, CMN enacted CMN Resolution No. 4,865/20, which frames regulatory sandboxes in the financial sectors regulated by BCB, CVM and SUSEP.[42]

BCB's sandbox principles were set by BCB Resolution No. 29/2020.[43] Participants licensed to operate in the BCB sandbox must carry out their transactions with integrity, reliability, security, and confidentiality, and implement structures for the risk management of the project under test.[44] Additionally, BCB Resolution No. 50/2020 sets the core regulation for the establishment, execution, and related procedures the first batch of companies engaged in financial and payment innovations.[45] The first batch of BCB's sandbox programme was launched in February 2021 and the final result of applications is expected to be disclosed in September 2021.

CVM's sandbox rules adopting its own regulatory safe harbour were established in May 2020 by CVM Instruction No. 626/20, later replaced in May 2021 by CVM Resolution No. 29/21.[46] 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. It also extended the deadline for analysis and selection of projects to September 30, 2021.[47]

SUSEP's sandbox framework, which focuses on the establishment of an open insurance environment, was adopted in March 2020 by Resolution No. 381/20,[48] recently amended by Resolution No. 417/21 in July 2021.[49] 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. They resulted in a number of new digital insurance products already offered to the public. Some of most celebrated innovative solutions covered telephone device thefts, car insurance on demand, and digital insurance brokerage companies. The second batch of SUSEP's sandbox programme was launched in late July 2021 and is expected to select around 15 new projects.[50]

Maybe the most noteworthy event in connection with regulatory sandbox development was the enactment in June 2021 of Supplementary Law No. 182/21 – the Brazilian Startups Law (*Marco Legal das Startups*).[51] Among a series of incentive provisions for newly established companies, it adopted a general framework for regulatory sandbox programmes.

Section 11 specifies that "*public regulators and agencies engaged in sectorial oversight and supervision may, independently or in collaboration with other agencies, exempt regulated entities, either individually or collectively, from specific regulatory requirements set forth*

within their legal mandate". On its turn, "experimental regulatory environments" are defined as "*sets of simplified special conditions for entities to receive temporary authorization from public regulators and agencies engaged in sectorial oversight and supervision, aimed to develop innovative business models and test experimental techniques and technologies, in accordance with simplified procedures setting forth compliance obligations and within the grounds established by such regulator and agency*".

Ownership and licensing requirements

CVM currently does not allow investment funds to directly purchase or invest in cryptocoins. These funds are regulated by CVM Instruction No. 555/2014 and, according to Circular Letter CVM/SIN No. 01/2018 issued in January 2018, these virtual assets may not always be qualified as financial assets.[52] 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, Circular Letter CVM/SIN No. 11/18 expressed allowed indirect investments in cryptocurrencies.[53] 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, which replicates the Nasdaq Crypto Index.[54] It was followed in July 2021 by the first Ethereum-based ETF, providing investors with safe custody and daily liquidity, but no concerns about private keys.[55]

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 the recommendation of the International Monetary Fund,[56] since August 2019, BCB has been classifying cryptocurrency mining activity as a productive process, and therefore considered non-financial assets produced, i.e., assets that have come into existence as outputs from production processes within the borders of a country.[57]

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 conduction of transactions exclusively through institutions authorised by BCB to operate in the exchange market.

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.[58] RFB Normative Ruling No. 1,888/19 requires cryptoasset exchanges to disclose specific transaction data from its clients, including information such as 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.

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.[59] 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 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 and House of Representatives Bill of Law No. 3,050/20. 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.gov.br/receitafederal/en/.
2. http://normas.receita.fazenda.gov.br/sijut2consulta/link.action?visao=anotado&idAto=100592.
3. https://www.bcb.gov.br/content/financialstability/paymentssystem_docs/Laws/Law12865.pdf.
4. https://www.bcb.gov.br/pom/spb/ing/Communique_25306.pdf.
5. https://www.bcb.gov.br/pom/spb/ing/Communique_31379.pdf.
6. http://otd.cpqd.com.br/otd/wp-content/uploads/2018/11/180629-E-Digital-English.pdf.
7. https://www.gov.br/governodigital/pt-br/EGD2020.
8. http://www.planalto.gov.br/ccivil_03/leis/leis_2001/l10332.htm.
9. https://www.gov.br/secretariageral/pt-br/noticias/2020/dezembro/destaques-do-governo-a-modernizacao-do-estado-e-a-vida-do-cidadao.
10. https://portal.tcu.gov.br/levantamento-da-tecnologia-blockchain.htm.
11. https://www.bcb.gov.br/en/about/cmnen.
12. https://www.bcb.gov.br/en.
13. https://www.gov.br/cvm/en.
14. http://www.susep.gov.br/english-susep/index.
15. https://www.bcb.gov.br/detalhenoticia/16776/nota.

16. https://www.bcb.gov.br/en/pressdetail/2337/nota.
17. https://www.serpro.gov.br/menu/noticias/noticias-2019/bconnect-uso-inicio-2020-blockchain-serpro.
18. http://www.planalto.gov.br/ccivil_03/_ato2019-2022/2020/decreto/D10550.htm.
19. https://www.in.gov.br/en/web/dou/-/portaria-n-108.092-de-20-de-agosto-de-2020-273476769.
20. https://www.bcb.gov.br/en/pressdetail/2397/nota.
21. https://www.bndes.gov.br/SiteBNDES/bndes/bndes_en.
22. https://www.bndes.gov.br/SiteBNDES/bndes/bndes_en/Institucional/Press/Noticias/2018/20180906_bndes_blockchain_bndestoken.html.
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. http://conteudo.cvm.gov.br/legislacao/instrucoes/inst588.html.
29. http://conteudo.cvm.gov.br/subportal_ingles/menu/international/ico_statement.html.
30. http://conteudo.cvm.gov.br/decisoes/2018/20180130_R1/20180130_D0888.html.
31. http://conteudo.cvm.gov.br/export/sites/cvm/noticias/anexos/2020/20201026_PAS_CVM_SEI__19957_003406_2019_91_relatorio_diretor_gustavo_gonzalez.pdf.
32. http://conteudo.cvm.gov.br/export/sites/cvm/sancionadores/sancionador/anexos/2020/SEI_19957003406_2019_91.pdf.
33. A comprehensive list of stop orders can be found at http://conteudo.cvm.gov.br/menu/investidor/alertas/alertas_deliberacoes_cvm.html.
34. http://www.mpf.mp.br/atuacao-tematica/sci/normas-e-legislacao/legislacao/legislacao-em-ingles/law-9-613-anti-money-laundering-law/view.
35. https://www.gov.br/coaf/en.
36. 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.
37. https://www.gov.br/coaf/pt-br/centrais-de-conteudo/publicacoes/guia-de-preenchimento-da-avec_2021_julho_2021.pdf.
38. 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://www.abcripto.com.br/autorregulacao-abcripto.
39. https://www.bcb.gov.br/en/pressdetail/2309/nota.
40. https://www.bcb.gov.br/estabilidadefinanceira/exibenormativo?tipo=Resolução%20BCB&numero=118.
41. http://www.planalto.gov.br/ccivil_03/_ato2019-2022/2019/lei/L13874.htm.
42. https://www.bcb.gov.br/content/config/Documents/Regulatory_Sandbox_Regulation_CMN_Resolution_No_4865_2020.pdf.
43. https://www.bcb.gov.br/content/config/Documents/Regulatory_Sandbox_Regulation_BCB_Resolution_No_29_2020.pdf.
44. https://www.bcb.gov.br/en/financialstability/regulatorysandbox.
45. https://www.bcb.gov.br/content/config/Documents/Regulatory_Sandbox_Regulation_BCB_Resolution_50_2020.pdf.
46. http://conteudo.cvm.gov.br/legislacao/resolucoes/resol029.html.
47. https://www.gov.br/cvm/pt-br/assuntos/noticias/cvm-conclui-etapa-do-processo-de-admissao-e-prorroga-prazo-para-analise.
48. https://www2.susep.gov.br/safe/scripts/bnweb/bnmapi.exe?router=upload/21939.

49. https://www2.susep.gov.br/safe/scripts/bnweb/bnmapi.exe?router=upload/25062.
50. http://novosite.susep.gov.br/noticias/susep-lanca-edital-para-segunda-edicao-do-sandbox-regulatorio-2/.
51. http://www.planalto.gov.br/ccivil_03/leis/lcp/Lcp182.htm.
52. http://conteudo.cvm.gov.br/legislacao/oficios-circulares/sin/oc-sin-0118.html.
53. http://conteudo.cvm.gov.br/legislacao/oficios-circulares/sin/oc-sin-1118.html.
54. http://www.b3.com.br/pt_br/noticias/b3-inicia-negociacao-do-primeiro-etf-da-hash dex.htm.
55. https://www.nasdaq.com/articles/ethereum-etf-to-list-on-brazils-stock-exchange-2021-07-14.
56. https://www.imf.org/external/pubs/ft/bop/2019/pdf/Clarification0422.pdf.
57. https://www.bcb.gov.br/content/statistics/externalsectorstatistics_prev/201908_External_sector_statistics_text.pdf.
58. https://www.gov.br/receitafederal/pt-br/acesso-a-informacao/perguntas-frequentes/declaracoes/dirpf/pr-irpf-2021-v-1-0-2021-02-25.pdf.
59. 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*) as at the time this chapter was drafted. Further information is available at https://www.tjsp.jus.br/Noticias/Noticia?codigoNoticia=63570.

Flavio Augusto Picchi
Tel: +55 11 2175 5025 / Email: flavio@fymsa.com.br

Flavio Augusto Picchi is a partner at FYMSA 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 start-up 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).

Luiz Felipe Maia
Tel: +55 11 2175 5025 / Email: maia@fymsa.com.br

Luiz Felipe Maia is a founding partner at FYMSA 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 the Getúlio Vargas Foundation, 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*.

FYMSA Advogados

Alameda Santos, 2.326, 1st floor, 01418-200 São Paulo, SP, Brazil
Tel: +55 11 2175 5025 / URL: www.fymsa.com.br

Canada

Simon Grant, Kwang Lim & Matthew Peters
Bennett Jones LLP

Government attitude and definition

Cryptocurrencies are not legal tender in Canada. Only coins issued by the Royal Canadian Mint and notes issued by the Bank of Canada are legal tender.[1] However, the Bank of Canada, the country's central bank, is experimenting with token-based digital currencies ("**CBDCs**"). Bank officials say that a CBDC "could be necessary to support the vibrancy of the digital economy by helping solve market failures and fostering competition and innovation in new digital payments markets".[2] The push to launch of a CBDC comes from two main factors: (i) a decline in the use of physical cash; and (ii) private currencies making serious inroads.[3] Although the Bank of Canada has not yet indicated when a CBDC could launch, the Bank's Deputy Governor said in February 2021 that "the [COVID-19] pandemic may bring us to a decision point sooner than we had anticipated".[4]

The Bank of Canada previously co-led an experimental project using distributed ledger technology to clear and settle payments (Project Jasper), leading to the release of four white papers.[5]

Cryptocurrency regulation

In Canada, cryptocurrencies are regulated primarily under securities laws as part of the securities regulators mandate to protect the public.

Sales regulation

Securities laws are enacted on a provincial and territorial basis rather than federally. The securities rules throughout the provinces and territories have largely been harmonised. The Canadian Securities Administrators (the "**CSA**"), an unofficial but influential organisation, represents all provincially and territorially mandated securities regulators in Canada.

Defining a "security"

The securities laws of a province or territory apply to people and entities: (a) distributing securities in that jurisdiction; or (b) from that jurisdiction. "Security" is broadly defined in Canadian securities legislation and covers various categories of transactions, including "an investment contract". The test for determining whether a transaction constitutes an investment contract, and therefore a security, for the purposes of Canadian securities laws was established by the Supreme Court of Canada, referring to U.S. jurisprudence. This test, the "**Investment Contract Test**", requires that in order for an instrument to be classified as a security, each of the following four elements must be satisfied:

(1) there must be an investment of money;
(2) with an intention or expectation of profit;

(3) in a common enterprise (being an enterprise "in which the fortunes of the investor are interwoven with and dependent upon the efforts and success of those seeking the investment, or of third parties"); and
(4) the success or failure of which is significantly affected by the efforts of those other than the investor.

Where the elements of the Investment Contract Test are not strictly satisfied, securities regulators in Canada consider the policy objectives and the purpose of the securities legislation (particularly protecting the investing public by requiring full and fair disclosure). The Supreme Court has stated that in determining whether a contract (or group of transactions) is an investment contract, substance, not form, is the governing factor.[6]

Regulator guidance

Securities regulators in Canada have issued many notices and statements regarding the potential application of securities laws to cryptocurrency offerings ("**CCOs**").

The CSA has said that a distribution not covered by the non-exclusive list of enumerated categories of securities in the *Securities Act* could still be subject to securities regulation if the offering otherwise falls within the policy objectives and purpose of securities legislation. In particular, many coin or token offerings, despite being marketed as software products, "should properly be considered securities … when the totality of the offering or arrangement is considered". In some circumstances, coins or tokens could also be derivatives subject to applicable legislative and regulatory requirements.[7]

The CSA has also said that platforms that facilitate the buying and selling or transferring of crypto-assets (collectively, "**CTPs**") trigger securities regulation, adopting the substance-over-form test in determining whether a crypto-asset that trades on a CTP is considered a security. If a CTP trades in crypto-assets that attach certain properties such as voting rights or rights to receive dividends, those assets will likely trigger securities regulation as they are already clearly defined as securities.[8] Additionally, if a CTP retains a purchaser's crypto-assets internally, such as through a virtual wallet (instead of making immediate delivery of an asset), those assets will likely be treated as securities.[9] The Ontario Securities Commission has recently initiated enforcement actions against several non-Canadian CTPs that accept Canadian customers without being registered in Ontario.[10]

Securities law requirements

In Canada, absent an available exemption: (a) a prospectus must be filed and approved with the relevant regulator before a person or entity can legally distribute securities; and (b) an individual or entity engaged in the business of distribution of securities, or advising others with respect to securities, is required to register with Canadian securities regulators.

A March 2021 notice from the CSA provided the following guidance on how cryptocurrency reporting issuers can meet their ongoing continuous disclosure obligations:[11]

(a) a description of the issuer's business, including its reliance on third-party service providers;
(b) risks to the issuer's business, specifically as they pertain to its crypto-assets;
(c) material changes to the issuer's business operations;
(d) the issuer's compliance with cryptocurrency accounting and auditing standards, policies, and related guidance, particularly as they pertain to cryptocurrency accounting, mining, valuation, and payments;
(e) the issuer's crypto-asset theft or loss prevention measures; and
(f) a statement disclosing whether the issuer utilises or relies on a crypto-asset trading platform to hold its crypto-assets.

If a material aspect of an issuer's business is investing in cryptocurrency or other crypto-assets, Canadian securities regulators may deem many of the investor protection considerations applicable to investment funds to be relevant to the issuer (such as requiring a qualified custodian), even if the issuer does not qualify as an investment fund.[12]

Legal status of CCOs in Canada

In order to determine whether a CCO constitutes a distribution of securities, Canadian securities regulators will perform a case-by-case, factual analysis, focusing on the substance and structure of the CCO rather than its form. Even if a CCO does not fall within the specific definition of a "security" provided by legislation, it may be found to involve the sale of securities if it otherwise triggers the policy objectives and purposes of securities legislation.

There are still ambiguities in cryptocurrency regulation; for example, with respect to crypto-assets such as non-fungible tokens and stablecoins.[13]

Applying the Investment Contract Test to CCOs

Statements from the CSA offer guidance regarding certain elements of a CCO that may increase the likelihood of the coins or tokens being found to be securities. While each offering of cryptocurrency should be analysed based on the particular circumstances of the offering and the features of the cryptocurrency, these statements, together with statements by U.S. securities regulators on the subject and decisions on the classification of CCOs such as the *Kik Interactive* decision,[14] offer insight into how the Investment Contract Test may be applied to CCOs.

Coins or tokens as securities

If a CCO is found to constitute a distribution of securities, it will trigger Canadian securities law requirements, including prospectus, registration, and continuous disclosure requirements, unless an exemption is available.[15] Individuals or businesses intending to rely on prospectus exemptions in connection with a CCO will need to satisfy the conditions for such exemption, including any applicable resale restrictions. Resale restrictions will be of particular concern if coins or tokens begin trading on cryptocurrency exchanges or otherwise in the secondary market following their initial sale. Issuers of a cryptocurrency that is a security will also need to comply with any applicable registration requirements (or registration exemption requirements), including dealer registration. Failure to comply with securities laws may result in regulatory or enforcement action by securities regulators against the parties behind the CCO, including fines and potential incarceration.[16]

Taxation

Background

The Canadian tax treatment of cryptocurrencies remains uncertain, with little legislative authority or administrative guidance. The Canadian federal tax authority (the Canada Revenue Agency, or "**CRA**") has expressed high-level views regarding the characterisation of certain payment tokens (*i.e.*, Bitcoin) and the potential income and sales tax implications of crypto mining and certain commercial transactions using tokens; however, these views are extremely limited.[17] Moreover, while the Canadian federal government has been making strides to address the void and clarify certain ambiguities, much work remains to be done in order to solidify the underlying tax regime.

Much of the analysis thus far concerning the potential tax treatment in Canada of cryptocurrency transactions is founded in an extrapolation of these administrative positions and thin legislative framework to scenarios upon which Canadian legislators and

tax administrators have not expressly considered. It is hoped that greater clarity will be provided in the near future that will not be limited to Bitcoin/payment instruments, but will also consider more recent developments in cryptocurrency technologies and their evolving distribution to, and usage by, the public, including initial coin offerings ("**ICOs**").[18]

Characterisation of cryptocurrency for income tax purposes

The CRA currently adopts the position that, despite its nomenclature, a cryptocurrency (specifically, a payment token such as Bitcoin) is not a "currency" for income tax purposes. Rather, such a cryptocurrency is akin to a commodity (albeit an "intangible"), the value of which will fluctuate based on external factors driven largely by investor sentiment and basic supply/demand. Based on this view, this type of cryptocurrency could potentially be analogised as the virtual equivalent of a precious metal such as gold or silver. Such a characterisation, if appropriate, could have significantly different tax implications under Canadian tax law as compared to "normal" cash (even foreign currency) transactions. Note that the CRA has generally been silent on its views concerning cryptocurrencies other than payment tokens (*i.e.*, Bitcoin). Accordingly, references below to "cryptocurrency" are generally restricted to payment tokens unless otherwise indicated.

(a) Acquisition of cryptocurrency

The threshold question is whether the initial acquisition of a cryptocurrency is a taxable event that potentially triggers a Canadian income tax liability to the person acquiring the cryptocurrency. The answer depends on the manner, purpose and circumstances in which the cryptocurrency is acquired.

The acquisition of cryptocurrency as a pure speculative investment, similar to physical gold or a publicly traded security, is generally not a taxable event to the person acquiring the cryptocurrency. However, the acquisition will establish the holder's "cost" in the cryptocurrency for Canadian tax purposes, which is relevant in the determination of the tax consequences that will be realised later when the cryptocurrency is eventually sold or otherwise exchanged.

This is to be contrasted with the acquisition of cryptocurrency as consideration for the provision of goods or services, or as compensation for some other right of payment. Such transactions are generally governed at this time by the CRA's position regarding "barter transactions", which is described in greater detail below under the heading "*Using cryptocurrencies in business transactions – Barter transaction*".

Where cryptocurrency has been acquired as a result of "mining" activities of a commercial nature, the current administrative position of the CRA suggests that the miner is subject to income tax at the time the cryptocurrency is earned. This is based on the concept that the mining activities are a service and that the mined cryptocurrency is received as compensation for those services. As with other services that are compensated with cryptocurrency, the CRA applies its position regarding barter transactions in determining the amount that is required to be included in income at the time the cryptocurrency is earned. This is an evolution of prior CRA administrative guidance regarding crypto mining, providing greater clarity regarding the quantum and timing of income recognition for miners.

(b) Determining a holder's tax cost in cryptocurrency

Once a cryptocurrency has been acquired, it will be important to determine its cost for Canadian tax purposes, which is a fundamental concept for determining the future income tax consequences on an eventual disposition of the cryptocurrency.

Where a cryptocurrency is purchased in exchange for Canadian currency, the cost of the cryptocurrency for income tax purposes will be equal to the amount of cash paid, plus any directly related acquisition expenses. If foreign currency is used, the holder will generally be required to convert the foreign currency into the Canadian-dollar equivalent at the applicable rate, pursuant to Canadian tax rules.

Cryptocurrencies can obviously be acquired by several alternative means, including commercial business transactions and other forms of "barter" exchanges. The particular facts surrounding any such acquisition could have meaningful distinctions regarding the determination of the holder's tax cost upon the acquisition of the cryptocurrency (see below, under the heading "*Using cryptocurrencies in business transactions – Barter transaction*").

(c) Tax on disposition of cryptocurrency

A person will realise taxable income (or loss) on an eventual disposition of a cryptocurrency. This includes a sale of the cryptocurrency for cash and the use of the cryptocurrency to pay for goods or services, or as consideration under other contractual rights/obligations (*i.e.*, a "barter transaction", described below).

If the cryptocurrency has a value at the time of its disposition in excess of its tax cost, it will be critical to determine whether the holder should report such excess as being on capital account (*i.e.*, a capital gain) or whether the proceeds should be reported as business income. This is a material distinction for tax purposes.

Generally, the buying and selling of cryptocurrencies can be regarded as being on capital account unless it is carried out in the context of a business of buying and selling such cryptocurrencies, or such buying and selling otherwise amounts to an "adventure or concern in the nature of trade". This is a factual, case-by-case determination requiring a detailed review of the holder's dealings with cryptocurrencies.

If a person acquires cryptocurrency as payment for goods or services in the normal course of the person's business (even if the person is not, *per se*, in the business of buying and selling cryptocurrencies as part of a speculative investment business), there is a risk that any appreciation realised when the person disposes of the cryptocurrency will be fully taxable as business income. Again, this issue is fact-dependent, should be reviewed on a case-by-case basis, and is described in greater detail below.

Using cryptocurrencies in business transactions

(a) Barter transaction

A person can accept a commodity in exchange for the provision of a good or service or as consideration for some other form of right of payment, with such transaction being subject to tax treatment under Canada's "barter transaction" tax rules.

In a barter transaction using cryptocurrency, the following must be considered by the person (referred to below as the "provider") that accepts a cryptocurrency as consideration in exchange for a good, service or other right:

- The provider will generally realise business income for Canadian income tax purposes equal to the fair market value of the goods, services or other rights provided (the "**Business Income Inclusion**"). For this purpose (but not for other purposes – see, *e.g.*, the sales tax implications described below), the value of the cryptocurrency at the time of the exchange is generally not the determining factor.
- The provider will generally acquire the cryptocurrency with a cost for Canadian income tax purposes equal to the Business Income Inclusion.

- The provider is now the owner of the cryptocurrency and must (eventually) do something with it, such as sell it to an investor or use it to purchase goods/services/rights in connection with its own business. Any gain or loss realised by the provider on an eventual disposition of the cryptocurrency (*i.e.*, the difference between the provider's cost in the cryptocurrency, and the amount received on the eventual disposition) will be taxable at such time to the provider. The issue then becomes whether such gain/loss is treated as being on full income account or on account of capital (the income tax treatment being materially different as between the two) (see the discussion above under the heading "*Characterisation of cryptocurrency for income tax purposes – Determining a holder's tax cost in cryptocurrency*"). Managing the provider's exposure to fluctuations in the value of the cryptocurrency post-acquisition will be a material and practical concern.

Another type of increasingly prevalent transaction (which may or may not be properly characterised as a "business transaction") is the acquisition by a person of one cryptocurrency ("**crypto #1**") in exchange for a different cryptocurrency ("**crypto #2**"). Such a transaction will also be considered a barter transaction involving the exchange of one commodity for another commodity. The person will generally be considered to have acquired crypto #1 with a tax cost equal to the fair market value of crypto #2 given up in exchange, computed as of the time of the barter transaction. The additional complication in this scenario is that the person acquiring crypto #1 will also be considered to have disposed of crypto #2, and will have to report any income/gain in respect of crypto #2 for Canadian income tax purposes (the person must therefore know his/her tax cost in crypto #2, which depends on the manner in which crypto #2 was originally acquired by such person).

(b) Sales tax implications

Canada imposes a federal sales tax (the goods and services tax, or "**GST**") on the supply of many goods and services, subject to detailed exemptions. Most Canadian provinces and territories also levy sales tax, which is often "harmonised" with the federal sales tax to effectively create one blended federal/provincial (or territorial) rate. Persons who are required to charge and collect federal GST (or harmonised sales tax) in respect of a business activity can generally claim a rebate in respect of such tax that the person directly incurs in the course of carrying on such business (generally referred to as an input tax credit, or "**ITC**"). The ITC mechanism is generally intended to mitigate the duplication of sales tax throughout a supply chain, and is designed to ensure that the cost of sales tax is ultimately borne solely by the end consumer of any particular good or service.

As with any provision of goods or services subject to federal and provincial/territorial sales taxes, a provider of goods/services that accepts cryptocurrency *in lieu* of government-issued currency must charge, collect and remit the appropriate sales tax. This may prove easier said than done in the context of cryptocurrency.

In this respect, the provider must be careful not to use the Business Income Inclusion amount (which is relevant under the Canadian tax authorities' current administrative policy to determine the provider's income tax associated with the sale) in determining the applicable amount of sales tax. For federal GST purposes, the Canadian tax authorities require that the provider charge, collect and remit GST based on the value of the cryptocurrency at the time of the sale. Presumably, the purchaser would be entitled to claim an ITC (if available) in respect of the full GST charged, if incurred in the course of a business activity.

While this may sound manageable at a high level, a few practical issues arise for the provider:

- How does the provider determine the value of the cryptocurrency at the precise moment of sale, particularly when cryptocurrencies are traded in non-traditional marketplaces and the value can swing wildly from day to day (possibly minute by minute)? What record-keeping is required by the service provider to justify the amount upon which it charges sales tax?
- How does the provider charge, collect and remit the sales tax in a transaction entirely handled in cryptocurrency, namely where the sales tax portion is also paid in cryptocurrency? The provider must remit to the Canadian tax authorities in Canadian currency (not cryptocurrency), meaning that the provider will be forced to either remit an equivalent amount of cash from other sources, or sell a sufficient amount of the cryptocurrency to generate the cash to satisfy the remittance. Given the volatility of most cryptocurrencies, an inherent risk is borne by the provider in collecting the sales tax in cryptocurrency.

Corporate directors are personally liable for any deficiencies in collecting or remitting sales tax. It is therefore critical for the provider of goods/services to take reasonable measures to ensure full compliance and mitigate any associated risk.

Another sales tax issue associated with transactions involving cryptocurrencies is whether the person disposing of the cryptocurrency (*e.g.*, the person using the cryptocurrency to purchase goods or services or trading one cryptocurrency for another) is required to charge and collect sales tax on the value of the cryptocurrency. In this respect, if the disposition of a cryptocurrency is a barter transaction akin to a disposition of a commodity, should such disposition be treated as a taxable supply of the cryptocurrency much in the same way as a commodity? If that were the case, compliance obligations and costs associated with routine cryptocurrency transactions could become exceedingly complex and beyond the reasonable abilities of many holders/users of cryptocurrency. In May 2019, the Canadian Department of Finance released draft legislation aimed at simplifying the federal sales tax on certain transactions involving "virtual payment instruments" ("**VPIs**"). In this respect, a VPI generally includes payment tokens such as Bitcoin, but expressly excludes tokens that operate in a manner similar to gift cards or that have functionality on a gaming or affinity/rewards programme platform. Pursuant to these proposals, transactions involving VPIs would generally be exempt from federal sales tax as a "financial instrument". These proposals, which have yet to be passed into law, demonstrate a willingness of the Canadian federal government to tackle the difficult tax and compliance issues associated with cryptocurrencies, albeit in only a fairly narrow and targeted manner at this time.

Money transmission laws and anti-money laundering requirements

Canada was the first country to approve regulation of cryptocurrencies in the context of anti-money laundering ("**AML**"). The *Proceeds of Crime (Money Laundering) and Terrorist Financing Act* ("**PCMLTFA**") includes virtual currencies through a framework for regulating entities "dealing in virtual currencies", treating them as money services businesses ("**MSBs**"). As MSBs, those dealing in digital currencies are subject to the same record-keeping, verification procedures, suspicious transaction reporting and registration requirements as MSBs dealing in fiat currencies.

In recent years, Canada has introduced a series of AML compliance measures that apply to MSBs, including MSBs dealing in virtual currencies. The definition of virtual currencies

in the PCMLTFA includes tokens that can be used either for payment purposes (such as Bitcoin or stablecoin) or for investment purposes (such as security tokens). Dealers that qualify as MSBs must register with the Financial Transactions and Reports Analysis Centre of Canada ("**FINTRAC**") and implement a complete AML compliance plan that is independently assessed.

Financial entities and MSBs are required to keep a record of electronic funds transfers executed cross-border and to include virtual currency transactions as well, meaning crypto-asset dealers that participate in cross-border transactions are subject to enhanced due diligence measures set out by the Act.

In July 2021, the requirement that MSBs report suspicious money transactions to FINTRAC and complete know-your-client ("**KYC**") verification when exchanging or transferring money was extended to virtual currency transactions. To comply with KYC obligations, MSBs and other reporting entities must: determine when a business relationship has formed and keep records of all business relationships; determine whether a client is a politically exposed person; verify beneficial ownership; and regularly monitor KYC information. MSBs are also required to maintain and submit transaction records to FINTRAC for Large VC Transactions: transfers of virtual currencies that exceed C$10,000 in a single transaction and transfers of virtual currency exceeding C$10,000 over multiple transactions in a 24-hour period.[19]

Promotion and testing

The CSA Regulatory Sandbox (the "**Sandbox**") was established to encourage the development of innovative products and services. The Sandbox allows companies engaged in cryptocurrency matters to register or seek exemptive relief (generally on a time-limited basis) in order to test products and services in the Canadian market. SN 21-327 expanded the application of the Sandbox to relevant crypto-asset trading platforms, including cryptocurrency trading platforms.

Once a company becomes a member of the Sandbox, it becomes subject to CSA surveillance and compliance reviews to ensure its continued eligibility for membership. While the majority of current Sandbox members are financial technology companies – including cryptocurrency issuers and trading platforms – the Sandbox is open to all companies with innovative business models.[20]

Ownership and licensing requirements

As noted above in "*Sales regulation – Securities law requirements*", an individual or entity engaged in the business of distribution of securities, or advising others with respect to securities, may be required to register with Canadian securities regulators. Similarly, investment fund managers are required to be registered.

On December 11, 2017, IIROC, the organisation that governs persons and companies registered under securities law, issued a notice to its members regarding margin requirements for cryptocurrency futures contracts that trade on commodity futures exchanges.[21] According to the notice, members are required to market and margin crypto futures contracts daily at the greatest of: (a) 50% of market value of the contracts; (b) the margin required by the futures exchange on which the contracts are entered into; (c) the margin required by the futures exchange's clearing corporation; and (d) the margin required by the Dealer Member's clearing broker.

As noted above in "*Sales regulation – Regulator guidance*", SN 21-327 and the framework in SN 21-329 subject CTPs to various existing securities rules. In particular, according to SN 21-329, the CSA anticipates that CTPs classified as Marketplace Platforms will eventually be subject to IIROC oversight.[22]

Mining

Because mining converts electrical energy (typically drawn from the power grid or a private power source) into waste heat in proportion to the difficulty of the underlying mathematical problem, it can result in large quantities of power being used for what may be perceived as a socially undesirable purpose. Furthermore, because mining enables the operation of a variety of cryptocurrencies (*e.g.*, Bitcoin), it functions as a convenient point for regulatory intervention. For those reasons, many official bodies have started to explore, or in some cases have implemented, laws or policies that contemplate cryptocurrency mining. In Canada, governmental regulators appear to have adopted a largely "hands-off" approach for the time being.

However, Hydro-Québec (a Québec Crown entity) recently announced the implementation of restrictions on energy allocation to 300 megawatts for users involved in cryptocurrency mining, the effect of which may be to discourage such activities in that province. We expect to see further intervention by government actors, as the quantity of power used by cryptocurrency mining operations, along with the use of various cryptocurrencies to facilitate illegal activities, continues to grow. To counteract the deleterious effects of such regulations on their operations, we additionally expect to see Bitcoin miners move to private power sources as time goes on.

Border restrictions and declaration

There are no border restrictions or declaration requirements as such.

However, as discussed above, dealers in crypto-assets that qualify as MSBs are now subject to the record-keeping requirements under the PCMLTFA, which requires these dealers to keep a record of the transfer with the personal information of both parties to the transaction, as well as being required to take reasonable measures to ensure that any transfer received includes such information.

Reporting requirements

See "*Money transmission laws and anti-money laundering requirements*", above. MSBs are required to send a large cash transaction report to FINTRAC upon receipt of an amount of C$10,000 or more in cash in the course of a single transaction, or upon receipt of two or more cash amounts of less than C$10,000 each that total C$10,000 or more if the transactions were made by the same individual or entity within 24 hours of each other.

Canadian resident taxpayers are required to file Form T1135 to the CRA if the total cost of their specified foreign property, including cryptocurrency held outside of Canada, exceeds C$100,000 at any point during the tax year.[23]

Estate planning and testamentary succession

Canada levies no separate estate tax, unlike many countries. However, a deceased is deemed to dispose of their property on death for its fair market value, which can result in income taxes being payable by the estate. Although it is far from settled, the CRA currently

takes the view that cryptocurrencies are generally commodities rather than currency, and that trading in cryptocurrencies will usually (with some possible exceptions) be regarded as being on capital account. In such circumstances, the estate will have to pay tax on any capital gains accrued as of the date of death. For a more detailed discussion of tax issues, see "*Taxation*", above.

In terms of estate planning, given the anonymous, decentralised nature of cryptocurrencies held on a blockchain, it will be imperative to include instructions on where to locate a copy of the private key related to the cryptocurrency. It would be unwise to include a private key in the will itself, since wills generally become public documents following probate.

* * *

Endnotes

1. *Currency Act* (Canada).
2. Bank of Canada, *The Positive Case for a CBDC*, Staff Discussion Paper 2021-11, July 20, 2021.
3. Bank of Canada, *Money and Payments in the Digital Age*, Remarks by Timothy Lane, Deputy Governor, CFA Montreal Fintech RDV2020, February 2020.
4. Bank of Canada, *Payments Innovation Beyond the Pandemic*, Remarks by Timothy Lane, Deputy Governor, Institute for Data Valorization, February 10, 2021.
5. https://www.bankofcanada.ca/research/digital-currencies-and-fintech/projects/.
6. *Pacific Coast Coin Exchange v Ontario Securities Commission* [1978] 2 SCR 112, at pages 127–129.
7. Canadian Securities Administrators, *CSA Staff Notice 46-307 Cryptocurrency Offerings.*
8. Canadian Securities Administrators, *CSA Staff Notice 51-363 Observations on Disclosure by Crypto-assets Reporting Issuers*.
9. *Ibid.*
10. https://www.bennettjones.com/Blogs-Section/New-Regulatory-Guidance-Requires-Immediate-Attention-from-Crypto-Trading-Platforms.
11. *SN 51-363*, at page 5.
12. *SN 51-363*, at page 6.
13. Ryan Clements, "Emerging Canadian Crypto-Asset Jurisdictional Uncertainties and Regulatory Gaps" (2021) 37:1 BFLR.
14. U.S. Securities and Exchange Commission, "SEC Obtains Final Judgment Against Kik Interactive For Unregistered Offering" (October 21, 2020), online: Press Release 2020-262 https://www.sec.gov/news/press-release/2020-262.
15. *Securities Act* (British Columbia) [BCSA], at s 61; *Securities Act* (Alberta) [ASA], at s 110(1); *Securities Act* (Ontario) [OSA], at s 53(1).
16. *BCSA*, at s 155; *ASA*, at s 194; *OSA*, at s 122.
17. Certain provincial tax authorities, namely Revenu Québec, have also published their own administrative positions on certain narrow issues (*i.e.*, provincial sales tax) dealing with cryptocurrencies.
18. The taxation of ICOs is beyond the scope of this chapter, due to: (i) the significant differences in potential ICO structures and legal characterisation of the underlying transactions; (ii) the speed at which ICO structure and cryptocurrency "technology"

and forms of offerings are evolving; and (iii) the lack of meaningful legislative, judicial or administrative guidance from a Canadian tax perspective. However, the fundamental "building block" tax concepts discussed in this chapter likely form the basis of the analysis underpinning certain of the discrete transactions and legal relationships created in many current ICO structures.

19. https://www.bennettjones.com/Blogs-Section/Changes-to-AML-and-Virtual-Currency-Regulations-for-Reporting-Entities-and-Money-Service-Businesses.
20. Canadian Securities Administrators, "CSA Regulatory Sandbox" (Undated), online: https://www.securities-administrators.ca/industry_resources.aspx?id=1588.
21. Investment Industry Regulatory Organization of Canada, IIROC Notice 17-0238 – Rules Notice – Guidance Note – 17-0238 – Rules Notice – Guidance Note – Margin requirements for cryptocurrency futures contracts (December 11, 2017).
22. *SN 21-329*, at pages 7 and 44–46.
23. See Canadian Revenue Agency Interpretation Bulletin 2014-0561061E5, *Specified Foreign Property*, April 16, 2015.

* * *

Acknowledgments

The authors thank Andrew Young and Duncan Pardoe for their assistance with this chapter.

Simon Grant
Tel: +1 416 777 6246 / Email: GrantS@bennettjones.com

Simon Grant is a co-head of Bennett Jones' cross-disciplinary Fintech & Blockchain practice group. Simon practises corporate law with an emphasis on financing transactions and financial regulation.

Simon regularly advises clients on financial regulation and compliance, including foreign financial institutions and fintech companies doing business in Canada.

He also routinely acts for credit providers, borrowers and sponsors on loan facilities, acquisition financings, project financings and capital markets transactions.

Kwang Lim
Tel: +1 604 891 5144 / Email: LimK@bennettjones.com

Kwang Lim is a member of the Fintech & Blockchain practice group. His business law practice includes corporate finance and M&A. He focuses on offering practical and strategic advice and facilitating opportunities for domestic and international clients, including entrepreneurs, start-ups, scale-ups, public companies, and broker-dealers across various industry sectors. Kwang also advises on securities law compliance and corporate governance issues.

Kwang is an adjunct professor at the Faculty of Law, University of British Columbia where he teaches the Business Law Capstone course.

Kwang obtained his Master of Laws at the University of California, Los Angeles with a specialisation in business law.

Matthew Peters
Tel: +1 416 777 6151 / Email: PetersM@bennettjones.com

Matthew Peters advises clients in various industries, including natural resources, manufacturing, financial services, telecommunications, pharmaceuticals and technology, in connection with international tax planning, domestic and cross-border mergers and acquisitions, corporate reorganisations, corporate finance, executive and employee compensation and various other tax matters. He has also represented clients before the Tax Court of Canada and the Federal Court of Appeal.

Matthew is a frequent speaker on international and domestic tax matters, and has written and presented papers at conferences and seminars across Canada and the United States. He is a member of the Canadian and Ontario Bar Associations, Canadian Tax Foundation, New York State Bar Association, American Bar Association and International Fiscal Association.

Bennett Jones LLP

3400 One First Canadian Place, P.O. Box 130, Toronto, ON, M5X 1A4, Canada
Tel: +1 416 777 4801 / Fax: +1 416 863 1716 / URL: www.bennettjones.com

Cayman Islands

Alistair Russell, Chris Duncan & Jenna Willis
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. a bonus or "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 amount, 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.

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.

Alistair obtained a Bachelor of Civil Law with distinction from Christ Church, University of Oxford, and an LL.B. with first-class honours from King's College London.

Chris Duncan
Tel: +1 345 749 2057 / Email: chris.duncan@careyolsen.com

Chris is counsel in the trusts and private wealth group of Carey Olsen in the Cayman Islands and the British Virgin Islands and advises on the full spectrum of private wealth matters from structuring and restructuring to disputes as well as a wide variety of matters involving digital assets and cryptocurrencies.

Chris was formerly with Mourant in Guernsey and AWS Legal in New Zealand.

Chris obtained a Bachelor of Laws and a Bachelor of Science (majoring in Chemistry) from the University of Otago.

Jenna Willis
Tel: +1 345 749 2053 / Email: jenna.willis@careyolsen.com

Jenna is a senior associate in the corporate and finance group of Carey Olsen in the Cayman Islands and advises on all aspects of finance, fintech, corporate law and restructuring and insolvency.

Jenna was formerly with Freshfields Bruckhaus Deringer in London and Blake, Cassels & Graydon in Toronto.

Jenna obtained a *Juris Doctor* with honours from Queen's University, and a B.Sc. in Mathematical Science *summa cum laude* from McMaster University in Canada.

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.

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 CySEC will publish the Registry online, it will be publicly available, and it will have the following information for each CASP:

(1) Name, tradename, legal form and legal entity identifier 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.

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 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. (ii) 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.

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, 1st Floor, Office 105, 1065, Nicosia, Cyprus
Tel: +357 22 256 882 / URL: www.papakyriacoulaw.com

France

William O'Rorke & Alexandre Lourimi
ORWL Avocats

Government attitude and definition

Government attitude

French government policy appears to be supportive of the development of cryptocurrency, provided that it is regulated. The central part of the current regime, implemented in May 2019 by the PACTE Law,[1] introduced a specific regulation for digital asset service providers ("**DASPs**") and initial coin offerings ("**ICOs**") in the French Monetary and Financial Code ("**MFC**"). The French Financial Markets Authority (*Autorité des marchés financiers*, or "**AMF**") is responsible for enforcing these regimes and publishing recommendations and guidelines.

One of the most demanding and comprehensive in the European Union, the French DASP regime is thus already in line with the future Markets in Crypto-Assets ("**MiCA**") regulation.[2]

The French authorities, especially the AMF and the banking authority (*Autorité de contrôle prudentiel et de résolution*, or "**ACPR**"), are highly qualified and interested in cryptocurrencies and tokens. They each have a Fintech department to welcome and assist innovative projects.

In terms of taxation, the government also showed early on its intention to regulate digital assets as appropriately as possible, bearing in mind their specific nature. As of 2019, the lawmaker has introduced a particular tax regime for digital assets.[3] France has thus become one of the few jurisdictions to neutralise the tax effects of exchanges between digital assets that no longer constitute a taxable event.

Recently, the National Assembly's Finance Committee chairman stated that he wanted to work with the government on tax incentives for digital asset holders to reinvest their capital gains in different sectors of the economy.[4]

Finally, digital asset actors are represented by the *Association pour le Développement des Actifs Numériques* ("**ADAN**"),[5] which organises regular conferences and meetings about this industry. This Association is in close contact with the regulators to support the regulation of the sector.

Definitions

Digital asset

French regulation provides a definition for digital asset divided into two subcategories:

- **utility tokens**, defined as "any intangible asset representing, in digital form, one or more rights which may be issued, recorded, stored or transferred by means of a shared electronic recording device (i.e. a blockchain) enabling the owner of the asset to be

identified, directly or indirectly".[6] The key notion of the definition is the representation of a right on the issuer to access to a service or a technology; and

- **cryptocurrencies**, such as Bitcoin and Ether, fall under the definition of virtual currency, i.e. "any digital representation of value which is not issued or guaranteed by a central bank or public authority, which is not necessarily attached to legal tender and which does not have the legal status of money, but which is accepted by natural or legal persons as a means of exchange and which can be transferred, stored or exchanged electronically".[7] It refers to any tokens corresponding to a means of exchange without necessarily representing a right on the issuer.

Electronic money

E-money is defined as "electronically, including magnetically, stored monetary value as represented by a claim on the issuer which 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".[8] The definitions of digital assets and e-money are mutually exclusive, as the AMF recently pointed out, since digital assets cannot represent a monetary value. This does not prevent certain cryptocurrencies from falling within the definition of e-money. The question of the legal status of stablecoins is still open in France.

Stablecoins

As a cryptocurrency is not necessarily attached to legal tender, stablecoins could fall within the scope of the digital asset definition. However, the banking regulator considers whether some stablecoins, especially "fiat-pegged" stablecoins (i.e. whose stable value is backed by a currency), could be classified as e-money.

Non-fungible tokens

There is no legal definition or position from the regulators on non-fungible tokens. However, they seem to be excluded from the digital asset scope as, firstly, they are non-fungible assets that cannot be used as units of account and therefore as a medium of exchange (cryptocurrency definition). Secondly, they do not access a specific service or technology (token), as they only represent an asset or an image. Legally, they exclusively confer a right of property on the underlying.

Security tokens

Security tokens represent financial instruments or have the same characteristics. The qualification of a security token is based on the European definition of a financial instrument, covering equity securities, debt securities, units in collective investment funds and financial contracts.[9] The absence of a legal entity (decentralised autonomous organisation, informal group) does not prevent requalification in security tokens in the presence of a *de facto* company.[10] The AMF has published several analyses on the compatibility of security tokens and security token offerings ("**STOs**") with financial laws. Most primary market financial regulations apply to security tokens as the Prospectus regulation may apply. However, as far as the secondary market is concerned, the concepts of "settlement" and "delivery" seem incompatible with security tokens, especially if they are listed. In addition, the requirement for identification of a "blockchain manager" and intermediation by a credit institution is not appropriate for security tokens and the underlying blockchain. Actually, there has never been a regulated STO in France due to regulatory obstacles.

Cryptocurrency regulation

Token sale (ICOs)

In France, the framework for the public offering of tokens (or ICOs) is particularly favourable to innovation. Indeed, token issuers have the choice to apply for an optional visa provided for by law in order to be included on the AMF's whitelist and benefit from communication advantages. Nevertheless, tokens offerings without a visa are authorised and subject to only a few regulatory constraints.

In order for the AMF to issue its visa, a number of conditions must be met to protect subscribers:

- structure: the issuer must be "constituted in the form of a legal person established or registered in France";[11]
- transparency: the offering must comply with a certain degree of transparency, which implies that the white paper must include a certain number of details (i.e. rights and obligations related to the token, number of tokens issued, issue price, discounts granted, etc.);[12]
- security: the issuer must implement a mechanism to "track and safeguard" the assets collected (this may be a conventional escrow system but also a multiple signature system (known as a "multisig"));[13] and
- anti-money laundering: since issuers receiving AMF approval are subject to anti-money laundering and countering the financing of terrorism ("**AML/CFT**") requirements, the visa is subject to the implementation of an adequate compliance system. This is one of the most restrictive aspects for issuers, and probably one of the most important for the regulator.

Digital asset services

In line with the Fifth Anti-Money Laundering Directive ("**AMLD5**"), crypto regulation focuses on AML/CFT obligations. The French regime applies to providers of digital asset services defined by the MFC: (1) custody of digital assets on behalf of third parties; (2) buying and selling digital assets in legal tender; (3) trading of digital assets; (4) operation of a trading platform between users; and (5) other services (reception and transmission of orders, portfolio management, financial advice on digital assets, etc.).

The regime is divided into two levels:

1. mandatory registration for the first four services, mainly focusing on the fitness and propriety of the main shareholders and managers as well as compliance with French AML/CFT requirements; and
2. an optional licence for all services, including the services subject to mandatory registration, providing for all the obligations applicable to traditional financial players: equity requirement or insurance; post-trade transparency; prevention of conflicts of interest; and IT security, etc.[14]

Mandatory registration

For the services concerned, the registration procedure takes the form of a file as described in the AMF Instruction.[15] The AMF is the applicant's single point of contact. An AMF officer follows the application through the entire procedure, including the discussion with the AML/CFT department of the banking regulator.

The maximum legal duration of the procedure is six months, although the regulator keeps control of the schedule. In practice, despite the large number of applications, the time required is close to six months for solid ones.

The illegal exercise of an activity subject to registration is punishable by two years' imprisonment and a fine of €30,000.[16] However, the AMF appears to favour blacklisting and the blocking of the website or mobile application in France to actors in violation of French law.[17]

Before targeting the French market, foreign DASPs are required to be registered with the AMF and have the ability to obtain the optional licence. Thus, they do not have to relocate their activities in France as long as they are incorporated in the European Union.

According to the AMF, foreign DASPs are considered to be targeting the French market when they present any of the following characteristics:[18]

- a physical facility in France, such as business premises, crypto ATMs, etc.;
- communication aimed at the French market via press, radio or the Internet, in particular, on social networks through invitations to events, targeted advertising, affiliation campaigns, advertising retargeting, etc.;
- their products and services are distributed through one or several distribution system(s) to customers residing or established in France; and
- a postal address, telephone number in France, or simply a .fr domain name.

Consequently, foreign DASPs wishing to actively address the French market, for example, by using the services of French influencers, partnerships with French media or through a distributor in France, will have to register with the AMF before offering the four digital asset services subject to mandatory registration.

Regarding the localisation of activity in France, the registration regime provides that the applicant only has to be established in a Member State of the European Union or the European Economic Area. Due to Brexit, applying with a British company is no longer possible.

This very flexible legal condition on paper is not applied by the regulator, which requires a minimal substance in France for foreign DASPs, preventing application with a shell company. In practice, it is highly advisable to (i) open a branch/subsidiary in France, (ii) appoint a country manager in position to ensure compliance with the DASP's obligations regarding French regulations, and (iii) ensure that a relatively precise outsourcing contract, to be provided to the regulator, is concluded between the approved French entity and the foreign operating entity of the DASP.

Optional licence

The licence (i) enables DASPs to use communication means to develop the activity more quickly on the market (direct client solicitation, sponsoring, patronage), and (ii) gives DASPs considerable advance on the forthcoming European MiCA regulation, which provides for a simplified procedure for DASPs that are already licensed so that they do not have to re-submit information and documents already requested at the time of their national registration in order to obtain European registration.

Foreign DASPs may obtain approval in France, but three main requirements are expected from providers in terms of the location of resources and operations. The AMF verifies that: (i) the entity is not a mere mailbox; (ii) it demonstrates a sufficient number of employees who provide, for France, commercial, control and support functions (these employees do not necessarily have to be established in France and may work within another entity of the group); and (iii) a relatively precise outsourcing contract is concluded between the approved French entity and the foreign operating entity of the DASP.

In addition, the conditions for issuing the optional licence, which depend in part on the nature of the activity carried out, are more extensive and demanding. In addition to complying with the conditions of the mandatory registration, DASPs must, *inter alia*: have professional liability insurance or minimum capital requirements based on various ratios; have adequate security and internal control arrangements; have a resilient and secure IT system; have rules for managing conflicts of interest; provide clear, accurate and non-misleading information to their clients; warn their clients about the risks associated with digital assets; make their pricing policies public; and have an effective complaint management policy, etc.

Personal data

In September 2018, the French *Commission Nationale de l'Informatique et des Libertés* published its analysis on blockchain. It considered that there are no major obstacles to applying the data protection obligations set by the GDPR for blockchain projects.

Investment funds

Alternative investment funds are authorised to manage digital assets with a cap of 20% of the funds under management.

Sales regulation

The sale of digital assets, especially promotional communication, is regulated under French law to protect investors. The regulation governs both unlicensed DASPs and token issuers without a visa from the AMF.

Firstly, it is prohibited for DASPs without the optional licence, even with a registration, to make:

- direct solicitation, by any means, to obtain an agreement on a service on the operation of digital assets;[19]
- "any direct or indirect advertising by electronic means whose purpose is to invite a person, by means of a reply or contact form, to request or provide additional information, or to establish a relationship with the advertiser, to obtain the advertiser's agreement to carry out a transaction"[20] relating to any service on digital assets; and
- "any sponsorship or patronage operation [...] when its purpose or effect is to advertise, directly or indirectly" a service on digital assets without authorisation from the AMF.[21]

Taxation

Income tax

As of 1 January 2019, a tax regime applies specifically to capital gains on digital assets realised by individuals.[22] This regime is only applicable to capital gains realised as part of an individual's private asset management. When buying and selling digital assets is carried out on a professional basis, the gains are subject to the progressive income tax rate in the category of industrial and commercial profits.

Under the regime for individuals, the annual overall capital gain from the sale of digital assets is taxed at a flat rate of 30%, in line with the tax rate for securities. The overall annual capital gain is equal to the sum of all capital gains deducted from all capital losses realised on taxable disposals of digital assets by members of the tax household.

A transfer of digital assets is taxable when its counterpart is not a digital asset. Thus, exchanges between digital assets do not generate any taxation, which is still a French specificity that allows for the smooth development of decentralised services (decentralised finance services in particular). However, the sale of digital assets against legal tender (euro,

dollars, etc.) or the purchase of a good (such as a Tesla) or a service (such as lawyers' fees) in digital assets is a taxable event.

The capital gain calculation method follows a particular logic. The capital gain is not equal to the difference between the sale price and the purchase price of the digital asset sold. The capital gain is equal to a fraction of the overall capital gain of the entire portfolio of digital assets (all cryptos included) equal to the fraction that the amount of the sale represents of the overall value of the portfolio. For example, the sale of 10% of the portfolio implies a taxation of 10% of the overall capital gain of the portfolio.

Capital gains are declared annually when filing an income tax return. Taxpayers are also required to declare accounts opened with digital asset trading platforms based outside of France.

Corporate tax

Clarifications have also been made for companies, although not all of the grey areas have yet been addressed.

In particular, the French Accounting Standards Authority (*Autorité des normes comptables*) has provided clarification on the accounting treatment of tokens held by companies.[23] A special "tokens held" account has been created in the category of cash instruments.

Gains on digital assets held are only accounted for when the tokens are sold and unrealised gains are not taxed at the end of the year. However, unlike the individual regime, exchanges between digital assets constitute a taxable event for corporate tax purposes.

The accounting and tax treatment of digital assets for companies will depend on the use of these assets by the company. For example, unlike digital assets acquired as part of a cash investment, a mining company or a broker will be able to account for them as stock and draw the consequences for tax purposes.

In addition, there are important clarifications regarding the accounting and tax framework for token sales. In summary, when the issuer of tokens makes an explicit or implicit commitment to subscribers to provide a good or service for the tokens, the sale proceeds are not taxed in the year of issuance but following token utilisation or during project development. These clarifications usually prevent all the funds raised in the context of an ICO from being considered as taxable turnover in the year of the operation.

VAT

Lastly, VAT application to various operations involving digital assets has also been clarified.

Firstly, the purchase or sale of digital assets used as means of payment has been exempt from VAT since the now famous *Hedqvist* decision issued in 2015 by the Court of Justice of the European Union.[24] Through a general ruling published by the French tax administration, this exemption has been explicitly extended to all digital assets and to transactions between digital assets.[25]

Secondly, regarding ICOs, the tax administration has specified that VAT is not applicable when there is a contingency on the existence of the counterparty to the subscription to the tokens, this contingency breaking the direct link between the subscription and the expected counterparty.[26] In other words, token sales to fund a project are only subject to VAT when the tokens issued by the company are used by their holders. On the other hand, the issuer is generally able to retain its right to deduct.

Finally, regarding mining, the administration has expressly specified that in the absence of individualised service, the operation is outside the scope of VAT. Thus, the gains made by miners are not subject to VAT, but they cannot deduct input VAT.[27]

Money transmission laws and anti-money laundering requirements

Money transmission laws

The execution of payment transactions, defined as the action of "paying, transferring or withdrawing funds, irrespective of any underlying obligation between the payer and the payee, initiated by or on behalf of the payer or by the payee", requires prior authorisation as a payment service provider. Otherwise, the provision of payment services is punishable by three years' imprisonment and a fine of €375,000.

According to the ACPR's interpretation, the collection of funds on behalf of third parties constitutes a payment service. More specifically, the ACPR considers, since January 2014, that "the intermediation activity consisting in receiving funds from the buyer of Bitcoins in order to transfer them to the seller of Bitcoins" constitutes a payment service characterised by a collection operation on behalf of a third party.

According to the regulator, collection on behalf of third parties characterises the provision of two of the payment services listed in article L. 314-1, II of the MFC (transposing the Second Payment Services Directive): on the one hand, the execution of transfer operations associated with the management of a payment account; and, on the other hand, the acquisition of payment transactions.

This position presents major difficulties for brokers offering the purchase and sale of digital assets and service providers operating a digital asset trading platform, and the two bases for treating collection on behalf of third parties as a payment service appear legally questionable.

AML/CFT requirements

French authorities regularly reinforce the AML/CFT requirements on digital assets based on the international (Financial Action Task Force, or "**FATF**") and European regulations (AMLD5) as well as the warning from Tracfin, the French financial intelligence unit.

According to the risk factors assessment, French regulation expects due diligence modulation based on the service offered, the client's characteristics and the source or destination country of the funds.

The level of AML/CFT control by the authorities depends on the digital asset services involved:

- for the services of custody and fiat-to-crypto, the AMF exercises an *a priori* check as part of the mandatory registration process; and
- for all the services subject to mandatory registration or under licence, the AMF or the ACPR will carry out *a posteriori* control to supervise the DASP's AML/CFT compliance in the course of their activities.

The French regulator's approach to AML/CFT follows the risk-based approach of the FATF guidelines, including its red flags list and the use of a blockchain analysis tool to help identify suspicious or unusual transactions.

France is quite strict in this respect, including reinforcement of the customer due diligence requirements since a Decree dated 2 April 2021:[28] the identification of all clients, even occasional ones, is now required without any transaction threshold.

Additionally, an asset-freezing mechanism shall be carried out by DASPs when detecting on the French national registry a person subject to a government asset-freeze measure: the DASP shall immediately notify this person to the authorities and freeze the assets involved.

Promotion and testing

Fintech support by the regulators

The AMF and the ACPR are the two competent regulatory authorities regarding Fintech projects.

The ACPR's FinTech Innovation Unit is dedicated to Fintech and financial innovation within the scope of banking services, e-money and payment services. This team acts as an interface between project sponsors and the ACPR-concerned departments. The ACPR studies new issues for financial regulation and supervision related to sectoral innovations (payment, banking, insurance) or more transversal innovations (blockchain, innovative use of data, artificial intelligence, connected objects, digital identity) and contributes to international work on Fintech and innovation, particularly that held within European and international financial regulatory bodies (Financial Stability Forum, Basel Committee, International Association of Insurance Supervisors, European Banking Authority, European Insurance and Occupational Pensions Authority).

The AMF has also set up a FinTech, Innovation and Competitiveness Division ("**FIC**"), which also serves as an entry point for innovative project leaders. In the last five years, this Division has developed significant expertise in projects involving digital assets.

Together, ACPR FinTech and AMF FIC run the FinTech Forum, which brings professionals together several times a year to discuss regulatory and supervisory issues relating to Fintech and innovation.

Public support for innovation

Companies in the digital assets sector are represented by ADAN, an association that aims to promote digital asset service development, by lobbying and publishing studies on the crypto environment (in relation to the banking sector, the impact of the COVID-19 crisis on the industry, etc.) and regulation (AMF/CFT, MiCA project, etc.).

Additionally, France offers numerous public aids for innovation players in the digital assets sector, under certain conditions:

- the *Banque Publique d'Investissement* is a public banking institution dedicated to supporting innovation and offers a wide range of aids: grants; bank guarantees; loans; and equity investments, etc.;
- the research tax credit (*Crédit d'impôt recherche*) allows the deduction of the research and development work carried out in France from corporate income tax; and
- the Young Innovative Companies status grants tax and social security exemptions.

Ownership and licensing requirements

Regarding the ownership of digital assets, including cryptocurrencies, they are characterised as intangible movable assets by the French courts.[29] In this regard, they may be subject to a proprietary right and related legal action as any other asset.

Licensing (mandatory registration or optional licence) is only required for DASPs as defined by the MFC. This shall not apply to a person making transactions of digital assets on its own account.

It should be highlighted that this licensing will not exclude other optional or mandatory authorisations such as the optional visa for ICOs, the intermediaries in a miscellaneous assets regime or the investment firm's licence to offer investment services on security token or crypto derivative products (swaps, futures, etc.).

Mining

Mining cryptocurrencies is permitted in France and does not fall into the existing French financial regulatory perimeter.

Border restrictions and declaration

There are currently no border restrictions or requirements to declare cryptocurrency holdings when entering France.

From a tax point of view, the exit tax system, which allows the French tax authorities to tax, under certain conditions, unrealised capital gains on securities portfolios in the event of a transfer of tax residence outside France, does not yet apply to digital asset portfolios.

Reporting requirements

AML/CFT legislation requires DASPs to submit suspicious reporting activity to Tracfin.

Estate planning and testamentary succession

French testamentary and inheritance laws do not provide for a specific regime for digital assets that, as intangible movable assets, are subject to inheritance tax.

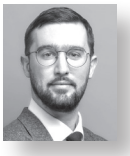
In practice, digital assets must be specifically mentioned in the will and declared by the testator. The public and private keys used to access the wallets must also be transmitted to the heirs, as well as a possible passphrase.

* * *

Endnotes

1. *Loi n° 2019-486 du 22 mai 2019 relative à la croissance et la transformation des entreprises, articles 85 et 86*.
2. Proposal for a Regulation of the European Parliament and of the Council on Markets in Crypto-assets, and amending Directive (EU) 2019/1937, Brussels, 24 September 2020 COM (2020) 593 final 2020/0265 (COD).
3. *Loi n° 2018-1317 du 28 décembre 2018 de finances pour 2019, article 41*.
4. E. Woerth, Amendment n° 417, 2021 finance bill, 8 June 2021 (see https://www.assemblee-nationale.fr/dyn/15/amendements_alt/4215/AN/417).
5. See https://www.adan.eu/en.
6. MFC, article L. 552-2.
7. MFC, article L. 54-10-1, 2°.
8. Directive 2009/110/EC of the European Parliament and of the Council of 16 September 2009 on the taking up, pursuit and prudential supervision of the business of electronic money institutions amending Directives 2005/60/EC and 2006/48/EC and repealing Directive 2000/46/EC (text with EEA relevance).
9. MFC, article L. 211-1 (see https://www.legifrance.gouv.fr/codes/article_lc/LEGIARTI000032469968/).
10. Civil Code, article 1873 (see https://www.legifrance.gouv.fr/codes/article_lc/LEGIARTI000006444477).
11. MFC, article L. 552-5.
12. MFC, article L. 552-4.
13. MFC, article L. 552-5.

14. AMF, Instruction DOC-2019-23, Rules applicable to digital asset service providers, 23 April 2021 (see https://www.amf-france.org/en/regulation/policy/doc-2019-23).
15. AMF, Instruction DOC-2019-23, Rules applicable to digital asset service providers, 23 April 2021 (see https://www.amf-france.org/en/regulation/policy/doc-2019-23).
16. MFC, article L. 572-23, al. 2 (see https://www.legifrance.gouv.fr/codes/article_lc/LEGIARTI000038509771/).
17. Recently, a major foreign player was blacklisted by the AMF. It was removed from this list once remedial measures were put in place.
18. RGAMF, article 721-1-1 (see https://www.amf-france.org/en/eli/fr/aai/amf/rg/article/721-1-1/20210523/notes).
19. MFC, article L. 341-1.
20. Consumer Code, article L. 222-16-1.
21. Consumer Code, article L. 222-16-2.
22. General Tax Code, article 150 VH *bis*.
23. ANC, *règl. n° 2018-07, 10 déc. 2018 modifiant le règl. ANC n° 2014-03, 5 juin 2014, relatif au plan comptable général modifié*.
24. ECJ, 22 October 2015, aff. C-264/14, *Skatteverket c/ David Hedqvist*.
25. BOI-RES-000054, *7 août 2019*.
26. *Ibid*.
27. BOI-TVA-CHAMP-10-10-10 § 60.
28. Decree of 2 April 2021 against the anonymity of virtual assets and strengthening the national system for combatting money laundering and terrorism financing, n° 2021-387.
29. Conseil d'Etat, 26 April 2018, n° 417809.



William O'Rorke
Tel: +33 7 49 23 69 17 / Email: william.ororke@orwl.fr

William O'Rorke manages ORWL Avocats' crypto and compliance practice. He holds a Master's degree in Corporate and Digital Law from the University of Paris I Panthéon-Sorbonne and has been a member of the Paris Bar since 2018. Previously, William developed the compliance department of Blockchain Partner, the leading French consulting firm, to assist its clients on the compliance of groundbreaking projects for large companies (60% of the CAC 40) and public entities (ANFR, *Banque de France*, and ADP). Meanwhile, William has developed an in-depth knowledge of the blockchain and crypto-assets sector: he is an active member of working groups (France Stratégie and Finance Innovation); and gives lectures at several universities, business schools and institutions (HEC, X, Paris II Assas, National Assembly and *Cour de cassation*). In 2020, he also co-authored the first law textbook on the legal issues of crypto-assets with LexisNexis.

Alexandre Lourimi
Tel: +33 6 60 30 09 67 / Email: alexandre.lourimi@orwl.fr

Alexandre Lourimi manages ORWL Avocats' tax and corporate law practice. After serving in the Versailles Administrative Court of Appeals dealing with corporate tax, VAT, and income tax controversies, Alexandre worked as a tax specialist in the Tax Controversy and Indirect Taxation department of Taj – Deloitte Société d'avocats. Specialised in digital tax issues, Alexandre has recognised expertise in the taxation of digital assets and blockchain projects. He regularly publishes in professional reviews, takes part in working groups on these matters, and speaks at various workshops and conferences. He is the co-author of the first French law book dedicated to the legal and tax framework of crypto-assets and blockchain.

ORWL Avocats

57 rue Réaumur, 75002 Paris, France
Tel: +33 9 77 19 63 07 / URL: www.orwl.fr

Gibraltar

Joey Garcia, Jonathan Garcia & Jake Collado
ISOLAS LLP

Government attitude and definition

The Government of Gibraltar has approached the growing cryptocurrency and wider blockchain and distributed ledger technology ("DLT")-related sector with a uniquely receptive and progressive attitude. Financial regulators and policymakers in Gibraltar have understood the need for regulation in this sector, responding rapidly to such demand as far back as 2014, with the creation of the Cryptocurrency Working Group. This private sector initiative led to the development of the Distributed Ledger Technology Framework ("DLT Framework"), which became effective on 1 January 2018, making Gibraltar the first jurisdiction in the world to deliver a framework of its kind that regulates businesses that use DLT for the defined purposes relating to a "storage" or "transfer" of "value", which is a wider concept than pure virtual assets. The DLT Framework currently includes nine principles that apply to DLT businesses operating in Gibraltar and these principles are substantiated by detailed guidelines constructed in a way that allows them to evolve at the same pace as the technology and its application, while always maintaining the core regulatory and legislative principles. The response to this approach has been global and truly significant. Those who know nothing about Gibraltar may be surprised, but those who know the history of the small jurisdiction, with a joined-up partnership between lawmakers, regulators and industry that is able to adapt and evolve to attract the right opportunities at the right level, with the speed and flexibility needed to accomplish such goals, will not be surprised at all.

This success has also been seen in the crypto funds space: pursuant to a 2020 research report into the global crypto hedge fund landscape, commissioned by PwC and Elwood Asset Management, Gibraltar was shown to be the third-highest jurisdiction of choice for crypto hedge fund managers (with 10% of crypto hedge fund managers based in Gibraltar), only behind the UK (15%) and the US (52%). Gibraltar was also listed as having the fourth-highest number of domiciled crypto hedge funds (6%).

More recently, the third annual edition of the report, published in 2021, shows Gibraltar as having strengthened its position as a preferred domicile for crypto hedge funds, with the third-highest number of domiciled crypto hedge funds (9%), overtaking the BVI (8%) and Luxembourg (3%), and pushing down Liechtenstein to less than 5%. Furthermore, the two leading jurisdictions for crypto hedge funds have experienced an overall decline in their market share compared to the 2020 report (the US from 38% to 33% and the Cayman Islands from 42% to 34%), whereas Gibraltar has maintained steady growth (from 6% to 9%).

Since the coming into force of the DLT Framework, the Government of Gibraltar has been delivering on a detailed and strategically formulated activity schedule, created to proactively drive home Gibraltar's very strong DLT message, by researching and identifying key markets and audiences and focusing its marketing in these areas. The Government of Gibraltar also

launched an advisory group that focuses on the creation of new technology-related education courses, such as blockchain. The New Technologies in Education ("NTiE") group, which is a well-established initiative since its inauguration in 2018, is a joint initiative between the Government and the University of Gibraltar in collaboration with some of the leading new technology companies based in Gibraltar. The advisory group's aim is to address the growing demand for related skills as the sector continues to expand in Gibraltar. The University of Gibraltar has also successfully been delivering a professional course in this space titled "Professional Certificate of Competence in Blockchain & Smart Contracts".

Whilst Gibraltar has shown leadership in this space, development is clearly an ongoing process and Gibraltar is aware of the importance, as a jurisdiction, for it to invest in supporting the development of knowledge and skills in tandem with generating economic results as it continues to strive for excellence. The Government of Gibraltar created the Gibraltar Association for New Technologies ("GANT") in 2018, an association formed together with the private sector, including Gibraltar's leading law firms, accounting firms and technology companies all forming part of its membership. GANT serves several purposes, primarily enhancing the development in Gibraltar of the use of blockchain and DLT and other future developments (collectively referred to as "New Technology"), with a view to enhancing the reputation, integrity and public trust in this sector.

GANT has also been tasked to raise the profile of "New Technology" in Gibraltar across a spectrum not necessarily limited to financial services. This includes encouraging respective organisations to emphasise the high value of their reputation and interest in contributing to enhanced client and investor protection and remaining committed to safeguarding customer and jurisdictional interests. GANT also provides a forum for discussion on "New Technology" issues within the membership and to assist other sectors of the wider Gibraltar Finance Centre, whilst also assisting and advising the Government of Gibraltar on all aspects of this sector.

Cryptocurrency regulation

In terms of the activity of the business in the DLT space, as highlighted above, Gibraltar has developed the first DLT-specific regulatory and principles-based legislative framework for these operators. This detailed framework goes well beyond the basic compliance requirements or registration processes that exist in many jurisdictions. Cryptocurrencies are not considered legal tender in Gibraltar and, accordingly, are not issued or guaranteed by the Government of Gibraltar.

While the United Kingdom and Gibraltar are no longer members of the European Union, subject to certain exceptions, all direct EU legislation and all EU-derived domestic legislation so far as operative immediately before midnight on 31 December 2020, continue to form part of Gibraltar's domestic legislation pursuant to ss5(1) and 6(1) of the European Union (Withdrawal) Act 2019. Accordingly, the provisions of all EU-derived financial services frameworks, as they stood at midnight on 31 December 2020, continue in force and effect in Gibraltar.

Therefore, as in most jurisdictions that operate under European law principles, depending on the construct of the virtual currency, cryptocurrencies may still qualify as electronic money ("E-Money"), as a form of asset-backed security, financial instrument or even unit of a collective investment scheme ("CIS") arrangement. Without being able to go into each of these for the purposes of this chapter, in the context of the recent focus on stablecoins and central bank-issued digital currencies, on a European level, the regulation of

E-Money is based on the E-Money Directive, which defines E-Money as an electronically, including magnetically, stored monetary value as represented by a claim on the issuer, which is issued on receipt of funds for the purpose of making payment transactions, and accepted by a natural or legal person other than the E-Money-issuer. This definition is in line with the definition contained in the Financial Services (Electronic Money) Regulations 2020. E-Money requires an issuer; therefore, a cryptocurrency that comes into existence by way of mining (e.g. Bitcoin) without an issuer, or representing any form of claim on any issuer, should not qualify as E-Money. Conversely, a cryptocurrency that is issued by an issuer at par value against fiat and furnished with the promise of the issuer to be redeemed in exchange for fiat against the issuer of that currency, and therefore being accepted as means of payment by third parties, would qualify as E-Money and trigger a number of considerations around this from a payments services perspective also.

Owing largely to the difficulty of regulating cryptocurrencies themselves, the DLT Framework has attempted not to enforce the regulation of cryptocurrencies, but instead to impose a regulatory regime for firms that carry on by way of business, in or from Gibraltar, the use of DLT for storing or transmitting value belonging to others. Accordingly, regulation will depend on what services a firm is providing customers in respect to their cryptocurrencies and whether this falls under the scope of regulation.

Because cryptocurrencies vary widely in design and purpose, it should be kept in mind that these may represent transferable securities or financial instruments, and their promotion and sale would already be covered by existing securities legislation in Gibraltar such as the Financial Services Act 2019 ("FSA"). Its classification as a security triggers various consequences; in particular, regulatory consequences. The requirement to issue a prospectus when offering securities publicly is only one example of such a requirement. A distinction must be drawn between the concept of a security on the one hand and a financial instrument on the other, with the latter being the broader term.

"Securities" are one of several sub-categories of financial instruments. Regulatory requirements may therefore also arise for non-securities that are classified as financial instruments. This includes the requirements arising under MiFID II, which, in addition to applying to businesses providing certain investment services or engagement in certain activities with clients in relation to financial instruments, also defines "financial instruments" in a wide form, including forms of commodity derivative contracts and arrangements that may apply to any asset or right of a fungible nature (under certain conditions).

If a cryptocurrency meets the MiFID II definition of a financial instrument, then a number of crypto-asset-related activities carried out by an exchange are likely to qualify as investment services/activities for which a licence is required outside of the DLT Framework. This includes multilateral trading facilities, organised trading facilities and other exchange-related activities.

Gibraltar is further looking to expand and extend the obligations to which DLT firms must adhere and is subsequently looking towards adding a 10th principle to the DLT Regulations with an aim to regulate and develop market integrity standards for crypto exchanges. The International Organization of Securities Commissions ("IOSCO") has identified several issues that merit consideration relating to transparency, custody, clearing and settlement trading, security and systems integrity. Implementing market integrity standards for these exchanges is one of the most pressing issues in the market, with organisations such as Bitwise and BTI estimating that 70–95% of all trading volume on exchanges is potentially manipulative. The effect of which is a reduction in market confidence in this sphere.

It should of course be borne in mind that foreign exchange markets, stock markets and commodity brokers face or have faced market risks in the past, but now fall squarely within developed rules and frameworks that prevent or restrict such manipulation taking place. This is not to say that there is no manipulation taking place in the more mainstream markets, but rather that it is less prevalent due to such regulation. Thus, the introduction of these standards in the regulatory sphere in Gibraltar would serve to restrict manipulation in the same way that this is restricted in traditional markets.

Sales regulation

It may be the case that tokens do not qualify as securities or financial instruments under Gibraltar or EU-derived legislation. Gibraltar also does not maintain separate classifications of virtual asset categories but, although the issuance of any token may not be captured within financial services legislation, from a compliance and risk perspective, any such creation and issuance will always be caught by the Proceeds of Crime Act ("POCA") in Gibraltar, which was specifically amended to capture this activity. Similarly, the operation of the actual business relating to such a token or virtual asset could also be captured within the DLT Framework, despite the issuance potentially not being captured. In the event that the token or assets do constitute securities, there is currently an EU-derived framework dealing with this, as has been described above. Accordingly, Gibraltar is not looking to introduce a framework that will modify, in any way, securities law or the EU Prospectus Regulation requirements. That is to say, the public offering of tokens that constitute securities does not require further regulation from a Gibraltar perspective and will continue to fall under current frameworks governing the issuance of securities.

It should also be noted that entities issuing tokens may separately have to comply with classic consumer protection law, depending on the design of the digital token.

Taxation

It should be noted that the treatment of cryptocurrencies is not specifically considered in current tax legislation in Gibraltar, nor in accounting standards that are generally accepted in Gibraltar; therefore, where relevant, general principles implicit in current legislation, and accounting standards that are believed to be appropriate, are applied.

In Gibraltar, there is no capital gains tax, value-added tax, death duties, inheritance, wealth, capital transfer, gifts, or withholding tax levied at present. For companies, corporation tax is generally 12.5%, payable on profits that derive from income accrued in or derived from Gibraltar; that is to say, by reference to the location of the activities that give rise to the profits. Under tax legislation, the location of the activities that give rise to the profits of a business whose underlying activity results in income, and requires a licence and regulation under any law of Gibraltar, shall automatically be considered to derive from Gibraltar. Favourable tax packages are also available for High-Net-Worth Individuals and High Executives Possessing Specialist Skills who want to establish residence in Gibraltar and can benefit from tax payable on income being restricted to a capped amount, which encourages talent towards Gibraltar.

Money transmission laws and anti-money laundering requirements

A DLT firm is caught as a relevant financial business ("RFB") under POCA in Gibraltar. Accordingly, a DLT firm is subject to know-your-customer and anti-money laundering ("AML") obligations. Furthermore, under the DLT Framework, a DLT firm "must have systems in place to prevent, detect and disclose financial crime risks such as money

laundering and terrorist financing". The requirement is derived from: EU Anti-Money Laundering Directives; POCA 2015; and the FFSC0 Anti-Money Laundering Guidance Notes. There are also additional and specific guidance notes relating to the "Financial Crime" factor, which have been prepared specifically for DLT firms to set out regulatory expectations.

Firms are required to establish procedures to: apply customer due diligence ("CDD") procedures; appoint a Money Laundering Reporting Officer to whom money laundering reports must be made; establish systems and procedures to forestall and prevent money laundering; provide relevant individuals with training on money laundering and awareness of their procedures in relation to money laundering; screen relevant employees; and undertake an independent audit for the purposes of testing CDD measures, ongoing monitoring, reporting, recordkeeping, internal controls, risk assessment and management, compliance management and employee screening. The frequency and extent of the audit shall be proportionate to the size and nature of the business.

It is possible for a DLT firm's compliance programme to use customer verification tools (such as Jumio) as well as blockchain technology (such as Coinfirm). As the DLT Framework is based on the application of principles rather than rigid rules, DLT firms are able to use innovative solutions provided they can satisfy the Gibraltar Financial Services Commission ("GFSC") that they meet its regulatory obligations.

The application of this AML regime to DLT firms has been seen by many as a precursor to the requirements under the EU's Fifth Anti-Money Laundering Directive ("AMLD5"), which has, for the first time, captured exchanges and pure custody wallet providers. Gibraltar-based businesses were already fully regulated and subject to such requirements as implemented by AMLD5 since the introduction of the DLT Framework, and so the introduction of AMLD5 has had no significant effect on those businesses operating from Gibraltar.

Gibraltar has also introduced the Proceeds of Crime Act 2015 (Relevant Financial Business) (Registration) Regulations 2021 ("RFBR Regs"), which impose an obligation on four classes of RFBs to register with the GFSC for the purposes of AML/CFT and counter proliferation financing supervision, to the extent they are not already supervised. In particular, these requirements apply to: (a) undertakings 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 DLT or a similar means of recording a digital representation of an asset; and (b) 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. Failure to register is a criminal offence punishable with up to two years' imprisonment and/or a fine. The registration regime should not be confused with any application for regulatory permissions required under the FSA, in respect of regulated activity defined under that Act. Such permissions would need to be sought if the RFB intends to carry out regulated activity.

Additionally, the registration requirements are not applicable where a person is already subject to supervision by a supervisory authority. The RFBR Regs provide fitness and propriety criteria that the GFSC will need to consider when accepting or refusing registration (including the withdrawal of registration after it is granted).

Gibraltar has included a definition for virtual asset service providers ("VASPs"), which replicates the Financial Action Task Force ("FATF") definition of the same. The only purpose of this definition is to define transactions between RFBs operating in Gibraltar and VASPs operating outside Gibraltar (and not therefore RFBs). Likewise, a definition of "virtual asset" is also used, which aligns with the FATF definition of the same.

Promotion and testing

Gibraltar has always maintained itself at the forefront of novel technological development. In fact, for most online gambling businesses around the world, it is found that most are based in Gibraltar, which was also the fastest mover in developing regulation around that space.

Gibraltar is hoping to replicate that philosophy in the blockchain space and follow the success of online gaming, and is doing so by stepping out of the regulatory "sandbox", in the same way as it did back in the gaming days. Rather than creating a "safe space" for businesses to test innovative financial products, services, business models and delivery mechanisms in a live environment without immediately incurring all the normal regulatory consequences of engaging in the activity in question, Gibraltar has instead chosen to provide legal certainty and allow businesses to operate within a purpose-built legislative framework. In doing so, it considers that a flexible, adaptive approach is required in the case of novel business activities, products and business models and that whilst regulatory outcomes remain central, these are better achieved through the application of principles rather than rigid rules. This is because, for businesses based on rapidly evolving technology, such hard and fast rules can quickly become outdated and unfit for purpose. Accordingly, Gibraltar's principles-based framework is based on risk and proportionality, and is outcome-focused yet robust.

The Government of Gibraltar recognises that this is a nascent industry and whilst Gibraltar has shown leadership in this space, development is clearly an ongoing process and Gibraltar is aware of the importance, as a jurisdiction, for it to invest in supporting the development of knowledge and skills, in tandem with generating economic results as Gibraltar continues to strive for excellence.

Ownership and licensing requirements

If a firm is engaging in an activity for business purposes, which involves the storage or transmission of cryptocurrencies belonging to third parties, it will need to be authorised under the DLT Framework.

If there is an intention to establish an arrangement that enables a number of investors to pool their assets and have these professionally managed by an independent manager, rather than buying investments directly as individuals, then CIS law is another relevant legal consideration.

The FSA defines a CIS 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 arrangement referred to above must be such that the participants in the arrangement do not have day-to-day control over the management of the assets. Further, the investments and the profits/income arising from them must be pooled, and/or the property managed as a whole.

There are two popular structures for setting up a CIS in Gibraltar: the Experienced Investor Fund ("EIF"); and the Private Scheme ("PS"). These structures are agnostic to the underlying assets they govern for investors.

Typically, a CIS that is to focus on crypto-assets would be best established as an EIF. Only when such a CIS is set up for a small group of persons previously known to each other, and where there will be no promotion of the CIS, would it be suitable to set up a CIS of

this nature as a PS. Indeed, the local Gibraltar Funds and Investments Association has published a draft code of conduct to this effect, which also serves as a reference point of elements that should be kept in mind when establishing funds dealing with crypto-assets. Among other things, the code will cover custody of crypto-assets, valuation, corporate governance and security.

The EIF is designed for professional, high-net-worth or experienced investors. Each investor would need to invest at least €100,000 in the EIF – or its equivalent in an alternative fiat – or prove a net worth of at least €1m, excluding one's personal residence.

The EIF regime is reliant on EIF Directors and other licensed service providers.

A CIS of this nature will fall within the definition of an alternative investment fund ("AIF") under the Financial Services (Alternative Investment Fund Managers) Regulations 2020. Accordingly, there will be multiple considerations that become relevant, both in terms of the sale, promotion and management of that AIF, as well as the depositary arrangements for AIF units.

Mining

The mining of Bitcoin and other cryptocurrencies is not covered by any specific legal or regulatory framework. Accordingly, it is permitted. As set out above, a cryptocurrency such as Bitcoin, which comes into existence by way of mining without an issuer, does not qualify as E-Money. However, this will ultimately depend on how the mining activity is conducted. For example, given the definition of an AIF, if the mining activities are conducted in a particular way that involves a collective group of people and shared infrastructure, an argument could certainly be made that the arrangement would qualify as a collective undertaking in the sense of the legal meaning.

Border restrictions and declaration

Presently, there are no border restrictions in place on declaring cryptocurrency holdings. Instead, these restrictions are usually in place for issues such as transport of goods. Though there are no restrictions in this sense, several of the above authorisation processes required by the regulations will require "mind and management" to be in Gibraltar, comprising an office with registered employees.

Reporting requirements

No specific reporting requirements are triggered for cryptocurrency payments made in excess of a certain value. However, any threshold amounts may determine the recordkeeping requirements that may apply to a business under POCA. Businesses under POCA must report suspicious activity of money laundering.

However, it is worth noting that in October 2018, the FATF amended its Recommendation 15 (New Technologies) of its 2012 Recommendations on International Standards on Combatting Money Laundering and the Financing of Terrorism & Proliferation ("FATF Standards") to explicitly clarify that the FATF Standards apply to financial activities involving "virtual assets" and added two new definitions relating to "virtual assets" and "VASPs". The FATF also began working on an Interpretative Note to Recommendation 15 to clarify the FATF Standards that apply to virtual assets and VASPs ("INR 15"), as well as Guidance for a Risk-Based Approach to Virtual Assets and Virtual Asset Service Providers ("VASP Guidance"), which explains how the FATF Standards apply to virtual assets and VASPs on a Recommendation-by-Recommendation basis.

Both the INR 15 and VASP Guidance were adopted by the FATF in June 2019, and clarified how the FATF Standards should apply, in particular in respect of the application of a risk-based approach to virtual asset activities and VASP operations, with supervision or monitoring for AML and combatting the financing of terrorism ("CFT") purposes, licensing or registration, preventative measures such as CDD, recordkeeping, suspicious transaction reporting and other sanctions and enforcement measures.

Without wishing to go into too much detail, it is important to note that while many jurisdictions took a reactive approach to the VASP Guidance and INR 15, beginning to take steps to comply with them after they were adopted in June 2019, Gibraltar had such measures in place since January 2018, well before the FATF introduced its VASP Guidance. Furthermore, in our view, Gibraltar's DLT Framework goes well beyond the FATF Standards in respect of the licensing and registration of VASPs. As a simple example, the VASP Guidance suggests that VASPs should be required to meet "*registration criteria set by relevant authorities*". The wording at paragraph 80 cites the fact that authorities should:

> "*[...] impose such conditions on licensed or registered VASPs to be able to effectively supervise the VASPs. Such conditions should allow for sufficient supervisory hold and could potentially include, depending on the size, nature of the VASP activities, requiring a resident executive director, substantive management presence or specific financial requirements*."

Gibraltar has also introduced various pieces of legislation, in part, to deal with the implementation of the "travel rule" prescribed under the revised Recommendation 15 (as read with Recommendation 16) of the FATF Recommendations. The "travel rule" obligations are now placed on RFBs, as defined in s.9 POCA, who send (on behalf of a "payer") or receive (on behalf of a "payee") virtual assets to or from VASPs.

The regulations operate by obligating the RFB acting for the payer in a virtual asset transaction that has been captured by the regulations, to obtain and submit certain information on the payer and on the payee. In many cases, the RFB may already have information on the payer as part of its CDD obligations under POCA, which apply to regulated DLT firms in Gibraltar, as well as other RFBs. However, unless the payee is also one of its clients, the originator RFB is unlikely to have information relating to the payee and will therefore need to have the relevant industry systems in place that allow this information to be securely provided.

The RFB receiving the virtual assets on behalf of the payee (which we can refer to as the "beneficiary RFB" for simplicity) has the obligation to ensure it receives the required information from the originator RFB and then corroborate this with its own records in respect of the payee's name and, where applicable, the payee's account number.

The information-gathering requirements shift slightly depending on whether the RFB is acting on behalf of a payer, a payee, or both (as well as on its own behalf). RFBs also have to consider the obligations when they receive virtual asset transfers from a person other than a VASP (e.g. virtual assets received from an unhosted wallet).

The travel rule does not apply where the RFB sends a virtual asset transfer to a person other than a VASP. In this case there are no information gathering requirements, other than the usual CDD requirements that an RFB has to meet under POCA. Given the overlap of travel rule information and CDD information obtained during the normal course of an RFB's activities, the regulations make clear that any requirement, under the regulations, for an RFB to obtain the information specified in r.4(2), or any part of it, shall constitute a CDD measure as if the requirement to obtain that information was listed in s.10 POCA. The recordkeeping requirements under s.25 POCA are also applicable to information obtained when sending or receiving virtual asset transfers.

Estate planning and testamentary succession

The law of succession in Gibraltar is largely based upon the UK Wills Act 1837, which is amended by Gibraltar's Wills Act. Administration of estates is governed by Gibraltar's Administration of Estates Act 1933, consolidated in 1948 (as amended).

The law of Gibraltar, as it relates to a deceased person who dies domiciled, closely resembles the laws of England & Wales. Moveable and immoveable property are treated differently. In the case of moveable property, the law of the country where the deceased died domiciled is applied.

There are no death duties to pay in Gibraltar.

Estate planning for cryptocurrency presents its own unique difficulties. Ordinarily, probate is a public process completed upon the presentation of various legal documents. Both of these concepts are in conflict with cryptocurrency.

Estate practitioners are going to have to be aware of the specific issues of cryptocurrency when drafting testaments, the aim being to ensure that the cryptocurrency property is accurately reflected, can be properly transferred upon the death of the holder, and also to ensure that the value of the property can be maintained.

As yet, there is no specific guidance issued in Gibraltar in relation to cryptocurrency and estate planning or succession.

Joey Garcia
Tel: +350 2000 1892 / Email: joey.garcia@isolas.gi

Joey is a corporate and fintech Partner at ISOLAS LLP. He worked closely with the Government of Gibraltar and the Gibraltar Financial Services Commission to shape the regulatory legislation for the use of Distributed Ledger Technology (DLT), and more recently in the transposition of the Travel Rule and the legislative gap analysis against FATF recommendations. He is recognised as a top 12 lawyer in the world in the field and has been appointed as a specialist lecturer on the topic at the University of Gibraltar.

Joey has also developed a strong international profile. Various prestigious memberships include the Wharton Reg@Tech think tank in Philadelphia, the Xapo representative on the Diem Association, and the Digital Chamber of Commerce in Washington. He also works as part of the United Nations ODC cryptocurrencies experts' workshop, and as a consultant to the UN in their discussions with regulators and law enforcement agencies from around the world in their VASP assessments. He also acts for some of the largest groups and platforms in the world in the blockchain space.

Jonathan Garcia
Tel: +350 2000 1892 / Email: jonathan.garcia@isolas.gi

Jonathan is a Partner at ISOLAS LLP, specialising in financial advisory services. He is a skilled advisor on collective investment schemes, investment managers, banks, e-money institutions and licensing and regulatory matters for blockchain start-ups. With over 10 years of experience as a financial services lawyer, his achievements saw him spend six months on a part-time secondment at the Gibraltar Financial Services Commission.

He is part of the Board of the Gibraltar Funds and Investments Association (GFIA), the local body representing the funds and investments industry, where he is responsible for managing a range of industry issues. Additionally, Jonathan has undertaken extensive work on international collective investment schemes, advising on solutions to a global client base of investment managers and banks.

Jake Collado
Tel: +350 2000 1892 / Email: jake.collado@isolas.gi

Jake commenced his training contract with ISOLAS LLP in September 2018, where he undertook seats in property, private client and corporate/commercial law. Having a particular interest in corporate and commercial matters, Jake spent the last few months of his training contract with the Financial Services team where he now sits as an Associate, having been admitted as a Solicitor to the Supreme Court of Gibraltar in 2019.

Jake is involved in assisting the Financial Services team in a range of matters including assisting in the licensing application process for Distributed Ledger Technology (DLT) Providers, as well as a number of DLT-related projects. He has also been involved in the setting-up and structuring of investment funds with a particular focus on corporate advisory and corporate structuring.

ISOLAS LLP

Portland House, Glacis Road, GX11 1AA, Gibraltar
Tel: +350 2000 1892 / URL: www.gibraltarlawyers.com

India

Nishchal Anand, Pranay Agrawala & Dhrupad Das
Panda Law

Government attitude and definition

Introduction

Presently, India has not enacted any special legislation for regulating cryptocurrencies or virtual currencies ("**VCs**"). The stance of the government towards cryptocurrencies will become clear only once the text to an impending bill titled *The Cryptocurrency and Regulation of Official Digital Currency Bill, 2021* ("**Proposed Bill**") is made available to the public. This bill will be the first step towards regulating the nascent, yet fast-moving, blockchain industry. Having said that, to understand the current attitude of the Indian government, we look below at the various positions it has taken over the years regarding cryptocurrency.

2013–2017

The first recognition by Indian law of the existence of cryptocurrencies came by way of circulars issued by the Reserve Bank of India ("**RBI**"), India's central bank, from 2013[1] through to 2017 ("**Warning Circulars**").[2,3] These Warning Circulars warned "*users, holders and traders*" of cryptocurrencies, including Bitcoin, about the potential financial, operational, legal, customer protection and security-related risks to which they expose themselves.

2018

The Finance Minister, in the union budget speech[4] for 2018–2019, made the government's position clear, stating that "*it does not consider crypto-currencies legal tender or coin and will take all measures to eliminate use of these cryptoassets in financing illegitimate activities or as part of the payment system*". This statement by the then Finance Minister has been often quoted in several responses given by the Ministry of Finance ("**MoF**") to parliamentary questions posed to it regarding the legality of cryptocurrencies.

Subsequent to the Warning Circulars, RBI issued a circular titled *Statement on Developmental and Regulatory Policies* on 5th April 2018 ("**Ring-Fencing Circular**")[5] directing all entities regulated by it, such as banks, non-banking financial companies and payment system service providers ("**Regulated Entities**"), to stop dealing in VCs or providing services for facilitating any person or entity in dealing with or settling VCs. Such services included maintaining accounts, registering, trading, settling, clearing, giving loans against virtual tokens, accepting them as collateral, opening accounts of exchanges dealing with them and transfer/receipt of money in accounts relating to the purchase/sale of VCs. RBI further directed all Regulated Entities that already provide such services to exit their relationships within three months from the date of the circular.

This Ring-Fencing Circular was challenged before the Hon'ble Supreme Court of India ("**SCI**") by way of a writ petition in 2018. This petition was decided in favour of the

petitioners on 4th March 2020 ("**SC Judgment**")[6] wherein the SCI set aside the impugned Ring-Fencing Circular on the grounds of proportionality.

2019

In February of 2019, a report titled *Report of the Committee to propose specific actions to be taken in relation to Virtual Currencies* ("**IMC Report**")[7] was published by an Inter-Ministerial Committee ("**IMC**") constituted by the government in November 2017 to study issues surrounding cryptocurrencies and propose potential actions. The salient features of the IMC Report are as under:

(a) The recognition of the disruptive power of Distributed Ledger Technologies on the economy as a whole, and the potential of "*non-official virtual currencies*" to destabilise India's economy. The easy violation of cross-border transaction norms using cryptocurrencies was also highlighted as a destabilising factor.
(b) The description of VCs as tradeable digital representations of value that function as: (a) a medium of exchange; (b) a unit of account; and/or (c) a store of value. However, as VCs lack any "*sovereign guarantee*", they were deemed incapable of being treated as money or legal tender.
(c) Distinguishing cryptocurrencies from VCs, noting that cryptocurrencies are a decentralised, cryptographic subset of VCs.
(d) The definition of a "token" as "*a utility, an asset or a unit of value issued by a company*", whose regulation may depend on the characteristics and the purpose for which they are issued. Tokens were further subdivided into "utility tokens" and "security tokens".
(e) The proposal for the creation of a Central Bank Digital Currency ("**CBDC**").
(f) The identification of the various risks consumers and citizens face from scams, negative financial and economic impact, and of the potential use of cryptocurrencies in committing crimes given their pseudonymous and cross-border nature.
(g) Arguably, the most salient feature of the IMC Report was the bill drafted and proposed by it, titled the *Banning of Cryptocurrency & Regulation of Official Digital Currency Bill, 2019* ("**Old Bill**").[8] In this bill, the IMC proposed a complete ban on mining, generation, holding, selling, dealing in, issuing, transferring, disposing of or using cryptocurrency in India. Fines and/or imprisonment of up to 10 years were proposed for certain violations of this ban.

2020

The following year, in 2020, the NITI Aayog, a public policy think-tank of the government of India, published the first of a two-part draft strategy paper titled *Blockchain: The India Strategy, towards Enabling Ease of Business, Ease of Living, and Ease of Governance* ("**Strategy Paper**").[9]

The Strategy Paper proposed a roadmap for broad adoption of blockchain technology for application in and to resolve business and governance process inefficiencies. The Strategy Paper recognised cryptocurrencies as token(s) that form an essential component of most public blockchains, and as a unique asset class that could denote ownership of the network (like shares of a company) and also form the basic unit of value exchange.

2021

Almost a year after the first part of the Strategy Paper was published, the Ministry of Electronics and Information Technology released its draft *National Strategy on Blockchain* in January 2021 ("**Draft Strategy**").[10] This Draft Strategy highlighted regulatory gaps in the legacy system to the widespread adoption of cryptocurrencies including: (i) the ambiguous nature of tokens; (ii) lack of Know-Your-Customer ("**KYC**") norms; (iii) non-inclusion in

the digital signature framework; and (iv) adequate provisions to data protection (including the right to be forgotten and localisation norms) as hurdles to mass adoption. It is expected that the Proposed Bill should address these matters particularly.

On 25th January 2021, RBI released a booklet titled *Payments and Settlement Systems in India, Journey in the Second Decade of the Millennium 2010–2020* ("**Booklet**"),[11] wherein it defined a CBDC as "*a legal tender and a central bank liability in digital form denominated in a sovereign currency and appearing on the central bank's balance sheet. It is in the form of electronic currency which can be converted or exchanged at par with similarly denominated cash and traditional central bank deposits*".

On 24th March 2021, the Ministry of Corporate Affairs issued a notification amending Schedule III of the Companies Act, 2013 ("**CA Amendment**").[12] Schedule III lays down the manner in which companies are required to prepare their profit and loss accounts and balance sheets for the purpose of submission to the government. The amended Schedule III specifically requires companies in India to disclose the following details:

(a) profit or loss on transactions involving cryptocurrency;
(b) amount of currency held as at the reporting date; and
(c) deposits or advances from any person for the purpose of trading or investing in cryptocurrency.

Responding to reports that certain banks were continuing to quote from RBI's earlier Ring-Fencing Circular, RBI issued a clarificatory circular dated 31st May 2021 ("**Clarificatory Circular**"),[13] wherein it clarified that banks and Regulated Entities were no longer bound by the Ring-Fencing Circular, as the same was not valid in view of the SC Judgment. It did, however, ask banks and other Regulated Entities to continue to carry out customer due diligence processes in line with regulations governing standards for KYC, Anti-Money Laundering ("**AML**"), Combatting the Financing of Terrorism ("**CFT**") and obligations of Regulated Entities under the Prevention of Money Laundering Act, 2002 in addition to ensuring compliance with relevant provisions under the Foreign Exchange Management Act, 1999 ("**FEMA**") for overseas remittances.

It can be seen when comparing the titles of the Old Bill and the Proposed Bill that the word "*banning*" has conspicuously been left out in the Proposed Bill. This, coupled with the Clarificatory Circular, is indicative of the government softening its stance towards cryptocurrencies in India.

RBI's CBDC

The IMC Report of 2019, deliberating on the major point of difference between fiat currency and VC, notes that while the former is expressly guaranteed by the central government, the latter has no such backing. In order for any VC to be declared legal tender, it will have to be expressly guaranteed by the central government. In that case, parties are legally bound to accept it as a mode of payment.

In line with the IMC Report and the Booklet, on 22nd July 2021,[14] the Deputy Governor of RBI in a public keynote address confirmed RBI's intention to introduce a CBDC. It was noted in the address that a CBDC would require an enabling legal framework as the current legal provisions have been created keeping paper money in mind. The Deputy Governor further noted that "*in modern economies, currency is a form of money that is issued exclusively by the sovereign (or a central bank as its representative). It is a liability of the issuing central bank (and sovereign) and an asset of the holding public. Currency is fiat, it is legal tender. Currency is usually issued in paper (or polymer) form, but the form of currency is not its defining characteristic*".

In this context, the Deputy Governor defined a CBDC as "*the legal tender issued by a central bank in a digital form. It is the same as a fiat currency and is exchangeable one-to-one with the fiat currency. Only its form is different*".

Subsequently, in an interview[15] with CNBC Asia, Singapore on 26th August 2021, the RBI Governor indicated that trials for a CBDC are scheduled to begin in December 2021. The focus when designing the CBDC would be security and integrity of the token. Further, the CBDC's impact on the financial sector, monetary policy and currency circulation are also being examined by RBI, as well as its foundational architecture (centralisation *versus* decentralisation, wholesale *versus* retail, forms of issuance mechanisms, etc.).

Parliamentary questions

In recent years, a slew of questions has been put by parliamentarians to the MoF, and the answers provided thereto provide insights on the government's attitude towards cryptocurrencies. A few takeaways from these recent responses given by the MoF are:

(a) the government is not tracking the number of "business companies" that have used cryptocurrencies for international transactions;[16]
(b) the government is currently relying on the Indian Penal Code, 1860 as the primary statute for protection of investors and traders in cryptocurrencies from frauds and other misdemeanors;[17]
(c) the government is not collecting data on the environmental impact of cryptocurrency mining;[18]
(d) the government is not currently tracking the number of cryptocurrency exchanges and investors linked to these exchanges; and
(e) the MoF also clarified that no information regarding the trafficking of drugs or laundering of money has come to the knowledge the MoF as at 27th July 2021.[19]

In a question asked to the Minister of Women and Child Development on sexual crimes against children, the Minister responded[20] that the government is contemplating AI-based cyber security measures to track the flow of cryptocurrencies, including on the dark web, by signing memorandums of understanding with industry partners and blockchain analysis companies for developing technological solutions. The primary focus of the government in this regard is to curb the use of cryptocurrencies in the purchase of child pornography online.

Cryptocurrency regulation

Cryptocurrencies are neither regulated nor prohibited. Individuals and entities are permitted to hold, invest in, and transact cryptocurrencies, provided they comply with existing laws while doing so. However, while dealing in cryptocurrencies, one must be mindful of the recent CA Amendment, as mentioned above, which brings in reporting requirements for companies. Further, any bank or other entities regulated by RBI will need to carry out due diligence processes in line with existing laws and regulations.

In a question[21] put to the Minister of Finance in the parliament of India, regarding the current regulatory regime surrounding cryptocurrency and its trading, the MoF reiterated the contents of the clarification issued by RBI in its Clarificatory Circular. Further, when questioned on the steps being taken to regulate cryptocurrencies, the Minister has on multiple occasions[22,23] replied with the following:

> "*The Government does not consider crypto-currencies legal tender or coin and will take all measures to eliminate use of these crypto-assets in financing illegitimate activities or as part of the payment system. The Government will explore use of block chain technology proactively for ushering in digital economy. A High-Level Inter-Ministerial*

Committee (IMC) constituted under the Chairmanship of Secretary (Economic Affairs) to study the issues related to VCs and propose specific actions to be taken in this matter recommended in its report that all private cryptocurrencies, except any cryptocurrency issued by the State, be prohibited in India. The Government would take a decision on the recommendations of the IMC and the legislative proposal, if any, would be introduced in the Parliament following the due process."

Another aspect of relevance is that in the Lower House/Lok Sabha's Bulletin dated 29th January 2021,[24] the introduction of the Proposed Bill is expected. The purpose of the Proposed Bill is to create a facilitative framework for creation of the official digital currency to be issued by RBI. The Proposed Bill also seeks to prohibit all private cryptocurrencies in India. However, it allows for certain exceptions to promote the underlying technology of cryptocurrency and its uses.

Though the text of the Proposed Bill is not in the public domain, it is anticipated that the regulations will seek to regulate based on different functions and uses of a cryptocurrency, and prohibit the use of cryptocurrencies as "currency" or "money", while permitting the use of cryptocurrencies for all other applications, where the cryptographic tokens issued do not encroach upon the domain of the Indian Rupee. This may be done by incentivising the blockchain industry to develop technology and cryptographic tokens that are unusable as currency.

In this context, it is apposite to quote from the SC Judgment of 2020, wherein it specifically highlighted the chimeric nature of cryptocurrencies, noting that:

"*6.62. It is clear from the above that the governments and money market regulators throughout the world have come to terms with the reality that virtual currencies are capable of being used as real money, but all of them have gone into the denial mode (like the proverbial cat closing its eyes and thinking that there is complete darkness) by claiming that VCs do not have the status of a legal tender, as they are not backed by a central authority.* ***But what an article of merchandise is capable of functioning as, is different from how it is recognized in law to be. It is as much true that VCs are not recognized as legal tender, as it is true that they are capable of performing some or most of the functions of real currency***."

One will have to wait for the release of the Proposed Bill to see how it reconciles cryptocurrency's money-commodity-security problem.

Sales regulation

India does not prohibit the sale and exchange of cryptocurrencies, and as noted above, there are also no specific laws enacted in India to regulate or prohibit the trade of cryptocurrencies or VCs. However, pieces of legacy legislation that deal with subjects such as: (i) trading and issuance of securities; (ii) trading of commodities; (iii) the 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 the cryptocurrency and its features will determine the regulatory mechanism that will be applicable to it, based on its categorisation as either an asset, commodity, security, store of value, etc.

If a cryptocurrency is used as a "store of value", e.g. Bitcoin, then these cryptocurrencies are freely tradable by individuals within India without any reporting requirements. Companies incorporated in India, on the other hand, are required to report any holdings in cryptocurrencies/VCs to the Ministry of Corporate Affairs as part of their annual returns. Such cryptocurrencies may come to be seen as either a commodity or an asset, which, if

purchased or sold by an Indian resident outside India, would attract exchange control norms notified under FEMA. It is presently unknown what categorisation may be given to crypto tokens under extant Indian law.

Where cryptocurrencies are issued by incorporated entities in India and such cryptocurrencies carry rights in the ownership or assets of such entities, such entities may be subject to rules regarding issue of securities, collective investment schemes and other like 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.

Trade of commodities and commodities exchanges in India are regulated by the Securities and Exchange Board of India ("**SEBI**"). Presently, VCs are not included in the definition of "commodities"; however, news reports indicate that an amendment in this regard may be likely.[25] This classification could impact crypto exchanges operating in India, bringing them under the purview of SEBI.

Guidance may also be taken from the way India imposes direct and indirect tax on both the sale of and the profits from the sale of cryptocurrencies in India, which is discussed in more detail in the Taxation section below.

Taxation

Profits and gains arising from the sale and trade of cryptocurrency would be exigible to tax in India. The Indian government collects tax revenue via both direct (Income Tax) and indirect (Goods and Services Tax or "**GST**") taxation. We will now look at the sources of profits from cryptocurrencies:

(1) **Mining/Staking/Airdrops**: Cryptocurrency can be generated or earned by a user by putting up its time and resources to a blockchain platform. This can in turn be traded by such users for consideration in the form of cash or other tangible or intangible goods.
(2) **Speculative Trade**: Several users purchase and acquire cryptocurrencies purely for the purpose of earning a profit from its sale. We will assume this includes all forms of derivative trading as well.

In both of the above cases, Income Tax and GST may apply as follows:

(1) **Income Tax**: Presently, cryptocurrency has not been categorised as an asset class or goods. Having said that, profits and gains from sale of cryptocurrency are exigible to Income Tax in one of two ways: (a) the law in India recognises software as "goods" and income arising out of sale of software can be considered business income and be taxed as such; and (b) the sale of any capital asset, in this case, cryptocurrency, would attract Capital Gains Tax. This would be established by assessing the period of holding, frequency of trading, size of holding as well as treatment in books of accounts.
(2) **GST**: The sale of goods in India is subject to GST at specified rates pertaining to the type of goods sold. Should cryptocurrency 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 revenue authorities. There is an additional onus on the parties to the transaction to seek registration as tax entities under the GST regime as well.

There remains, of course, the matter of cross-border cryptocurrency transactions and the related interplay between withholding tax and double taxation avoidance agreements. The movement of crypto tokens across borders, to and from wallets and exchanges poses an unresolved legal challenge on how to accurately tax the sale of cryptocurrencies internationally.

Money transmission laws and anti-money laundering requirements

Apart from the various RBI Circulars mentioned above, there are no specific laws regulating or prohibiting the transmission of cryptocurrency. Owing to the pseudonymised nature of transactions related to cryptocurrency, RBI via its Ring-Fencing Circular intended to put a complete prohibition on dealing in VCs. The Ring-Fencing Circular was subsequently struck down by the SCI and superseded by the Clarificatory Circular (discussed above), allowing Regulated Entities to deal in cryptocurrencies subject to compliance with the existing KYC, AML and CFT requirements.

While the Clarificatory Circular issued by RBI may only apply to Regulated Entities, it is advisable for any entity including those providing services related to cryptocurrency (including crypto exchanges) to comply with the said obligations. Compliance will enable the said entities to assist enforcement agencies with their investigation and absolve themselves of any direct liability. Enforcement agencies in India have acted against parties in violation of the AML laws while dealing in cryptocurrency.[26]

Further, the use case of the cryptocurrency may also play a determinant factor in identifying the money transmission laws applicable to it:

(1) **Store of Value**: RBI guidelines as stated above will apply. With the Indian government and RBI seriously mulling over a CBDC, it seems unlikely that other cryptocurrencies will be accepted as a "store of value" or legal tender in India.

(2) **Utility Token**: This form of cryptocurrency can be used to avail goods and services offered on a proprietary platform. The value of the tokens is usually pegged to the actual monetary value of the goods and services being offered on the platform. Utility tokens may assume the role of prepaid payment instruments ("**PPIs**") and, depending upon whether the PPI system is a closed, semi-closed or open system, the relevant provisions of the Payment and Settlement Systems Act, 2007 along with RBI Circulars on PPIs[27] may become applicable.

(3) **Commodity or Security Token**: In case the cryptocurrency is treated as a commodity, the guidelines with respect to KYC, AML and CFT[28] issued by SEBI will become applicable. Currently, the list of commodities that can be traded under SEBI's aegis does not include cryptocurrencies in any form or manner.[29] However, there has been a great push by the industry viewing SEBI as the ideal body to regulate cryptocurrencies in India.[30] This view may also be reflected in the Proposed Bill.[31]

Promotion and testing

On 13th August 2019, RBI issued the *Enabling Framework for Regulatory Sandbox* ("**Framework**")[32] to promote the adoption and implementation of new technologies in the fintech space in India. The Framework currently includes "*Applications under block chain technologies*" in the indicative list of innovative technologies that may be experimented upon 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.

On 17th April 2020, SEBI issued a notification under the SEBI (Regulatory Sandbox) Regulations, 2020[33] grating relaxation on the enforcement of the other regulations "*for furthering innovation in technological aspects relating to testing new products, processes, services, business models, etc. in live environment of regulatory sandbox in the securities markets*". In August 2020, the Insurance Regulatory and Development Authority of India also came up with a regulatory sandbox "*to carve out a safe and conducive environment to experiment with innovative approaches (including Fin-Tech solutions)*" in the insurance

sector.[34] Unlike the RBI Framework, there is no specific inclusion or exclusion of crypto assets, VC or blockchain in either of these sandboxes. Each application under the respective sandbox is reviewed on a case-by-case basis by the respective regulatory body.

Nevertheless, once the much-anticipated Proposed Bill is introduced, implemented, and the government body(ies) responsible for regulating cryptocurrencies is (are) identified, it may become necessary to specifically provide for a regulatory sandbox for cryptocurrency to keep on par with international and domestic developments in this space.

Ownership and licensing requirements

In India, the activities of investment advisors and fund managers 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 crypto assets, the list of commodities that managers and advisers can deal in has been notified by SEBI[35] and does not include cryptocurrencies/VCs. Therefore, any investment advisers or fund managers currently providing services related to cryptocurrencies/VCs in India are doing so in their personal capacity and not as advisers or managers licensed by SEBI.

However, investment advisory companies and wealth management companies in India would mandatorily need to disclose their holdings and ownership of cryptocurrencies/VCs to the government of India from the current financial year onwards owing to the CA Amendment. This may not be applicable to individual advisers and fund managers.

Mining

Mining cryptocurrencies in India is not prohibited, regardless of the cryptocurrency being mined. There are also no regulations regarding mining cryptocurrencies.

To understand the government's attitude towards mining, reference may be made to the IMC Report. The IMC Report only highlighted the resource-intensive nature of mining non-official VCs, which it noted could lead to unfavourable long-term economic consequences.

Further, in the Old Bill proposed in the IMC Report, a "miner" is defined as "*a person who engages in mining of a Cryptocurrency*" and "mining" is defined as "*an activity aimed at creating a Cryptocurrency and/or validating a transaction of Cryptocurrency between buyer and seller of Cryptocurrency*". As noted above, the Old Bill also proposed to ban the mining of cryptocurrencies in India.

The Strategy Paper defines mining slightly differently, however, as "*the actions nodes take to authenticate transactions. Miners are economically incentivized to spend resources for maintaining the network by a reward of tokens which are generated by the distributed network*".

Given the fact that mining is neither regulated nor prohibited, all individuals and entities earning cryptocurrencies by mining will have to comply with existing laws that impact mining.

At present, we can divide mining into two main categories, namely: (a) institutional-level mining; and (b) hobbyist mining. To be able to set up a commercial cryptocurrency mining operation in India, the entity 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. However, regulating and/or outright banning of mining at an individual level would be challenging to say the least, since consumer-grade computer peripherals

(including GPUs and ASICs), which are available at retail prices in India, are capable of mining cryptocurrency efficiently. Banning the import of such computer peripherals by the Indian authorities could be in violation of international trade agreements.

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 particularly:

(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 cryptocurrencies under Indian law as either a capital asset or good, the applicable legislation may be triggered. This would require each cross-border transaction in cryptocurrencies 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 cryptocurrency transactions except in two circumstances: firstly, reporting of any income or profits from cryptocurrency in the Income Tax returns; and secondly, as required by the CA Amendment.

This leaves a significant gap in the regulatory landscape in India *viz*. AML, CFT and tax evasion. Platforms are seen to mitigate this by pre-emptively requiring users to undergo a KYC process. This may make it easier for authorities to trace large transactions in the future. Peer-to-peer sales, however, remain unchecked.

Estate planning and testamentary succession

There are no specific laws or regulations regarding the treatment of cryptocurrencies 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 the cryptocurrencies to his intended beneficiaries. This right may flow through a will, or through operation of law in the event the owner of the assets dies intestate.

The second aspect to consider is the manner in which the right to the cryptocurrencies devolves upon the beneficiaries. The primary challenge, as it exists today, is to enforce and/or exercise the right bequeathed to a beneficiary over cryptocurrencies.

In case of wills, to ensure that beneficiaries receive all cryptocurrency 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 the cryptocurrencies 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.

Endnotes

1. https://rbidocs.rbi.org.in/rdocs/PressRelease/PDFs/IEPR1261VC1213.PDF.
2. https://rbidocs.rbi.org.in/rdocs/PressRelease/PDFs/PR205413F23C955D8C45C4A1F56349D1B8C457.PDF.
3. https://rbidocs.rbi.org.in/rdocs/PressRelease/PDFs/PR15304814BE14A3414FD490B47B0B1BF79DDC.PDF.
4. https://www.indiabudget.gov.in/budget2018-2019/bspeecha.asp.
5. https://rbidocs.rbi.org.in/rdocs/notification/PDFs/NOTI15465B741A10B0E45E896C62A9C83AB938F.PDF.
6. https://main.sci.gov.in/supremecourt/2018/19230/19230_2018_4_1501_21151_Judgement_04-Mar-2020.pdf.
7. https://dea.gov.in/sites/default/files/Approved%20and%20Signed%20Report%20and%20Bill%20of%20IMC%20on%20VCs%2028%20Feb%202019.pdf.
8. https://prsindia.org/billtrack/draft-banning-of-cryptocurrency-regulation-of-official-digital-currency-bill-2019.
9. https://www.niti.gov.in/sites/default/files/2020-01/Blockchain_The_India_Strategy_Part_I.pdf.
10. https://www.meity.gov.in/writereaddata/files/NationalStrategyBCT_%20Jan2021_final.pdf.
11. https://rbidocs.rbi.org.in/rdocs/Publications/PDFs/PSSBOOKLET93D3AEFDEAF14044BC1BB36662C41A8C.PDF.
12. https://mca.gov.in/bin/ebook/dms/getdocument?doc=MjU4MzU=&docCategory=Others&type=open.
13. https://rbidocs.rbi.org.in/rdocs/notification/PDFs/45VIRTUALCURRENCIES37FE644EF97F4A36AAB951C73A411E96.PDF.
14. https://rbidocs.rbi.org.in/rdocs/Speeches/PDFs/CBDC22072021414F2690E7764E13BFD41DF6E50AE0AE.PDF.
15. https://rbi.org.in/scripts/BS_SpeechesView.aspx?Id=1119.
16. https://pqars.nic.in/annex/253/A51.pdf.
17. http://164.100.24.220/loksabhaquestions/annex/176/AU2138.pdf.
18. http://164.100.24.220/loksabhaquestions/annex/176/AU3412.pdf.
19. https://pqars.nic.in/annex/254/AS79.pdf.
20. https://rajyasabha.nic.in/rsnew/Questions/QResult.aspx.
21. http://164.100.24.220/loksabhaquestions/annex/176/AU2138.pdf.
22. http://164.100.24.220/loksabhaquestions/annex/176/AU3412.pdf.
23. https://pqars.nic.in/annex/253/AU3105.pdf.
24. http://loksabhadocs.nic.in/bull2mk/2021/29012021.pdf.
25. https://www.sebi.gov.in/legal/circulars/sep-2016/list-of-commodities-notified-under-scra_33359.html.
26. http://www.uniindia.com/ed-arrests-a-crypto-currency-trader-under-pmla/india/news/2260925.html and https://www.thestatesman.com/business/ed-grills-raj-kundra-bitcoin-pmla-case-shilpa-shetty-1502644694.html.
27. https://www.rbi.org.in/Scripts/BS_ViewMasDirections.aspx?id=11142.
28. SEBI (KYC Registration Agency) Regulations, 2011 and https://www.sebi.gov.in/legal/master-circulars/jul-2018/guidelines-on-anti-money-laundering-aml-standards-and-combating-the-financing-of-terrorism-cft-obligations-of-securities-market-intermediaries-under-the-prevention-of-money-laundering-act-2002-a-_39431.html.

29. https://www.sebi.gov.in/legal/circulars/sep-2016/list-of-commodities-notified-under-scra_33359.html.
30. https://www.moneycontrol.com/news/business/markets/cryptocurrency-exchanges-say-sebi-or-a-new-entity-not-rbi-should-regulate-the-sector-report-6906961.html.
31. https://m.economictimes.com/news/economy/finance/virtual-currencies-govt-plans-to-bring-a-bill-cryptos-to-be-treated-as-commodity/articleshow/85885645.cms.
32. https://rbidocs.rbi.org.in/rdocs/PublicationReport/Pdfs/ENABLING79D8EBD31FED47A0BE21158C337123BF.PDF.
33. https://www.sebi.gov.in/legal/regulations/apr-2020/securities-and-exchange-board-of-india-regulatory-sandbox-amendment-regulations-2020_46757.html.
34. https://www.irdai.gov.in/ADMINCMS/cms/frmGeneral_Layout.aspx?page=PageNo4224.
35. 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. Karan Khanna to this chapter.

Nishchal Anand
Tel: +91 98 9912 1634 / Email: nishchal@legalpanda.in

Nishchal is an intellectual property and technology law attorney practising in New Delhi since 2009. Besides representing large corporations in contentious IP and data protection matters, he regularly advises tech companies and start-ups on legal and regulatory compliance including IP structuring, product structuring and data compliance. Nishchal has been a 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 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 start-ups 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 a litigator practising in Delhi and Guwahati for over 12 years. His technology practice is focused on cryptocurrency and blockchain regulations, structuring of novel digital assets and tokens, and the integration of emerging technologies with traditional legal and business models, where his traditional practice is focused on corporate dispute resolution, securities laws, corporate insolvency and resolution, competition law, and banking laws. 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 and definition

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 Irish 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**). In its "Action Plan for 2021", launched under the IFS2025, the Irish Government committed to establishing a new Department of Finance Fintech Working Group. The Working Group will develop Ireland's policy positions in response to the EU's Digital Finance Package, coordinate the approach to fintech across the Department, and will engage with external stakeholders to encourage collaboration between policymakers and the fintech community. The Irish Government also committed to establishing an "Expert Group on Future Skills Needs", which will conduct a study to assess the additional skills required to exploit opportunities in subsectors such as fintech and blockchain, to be finalised in 2022.

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. The Central Bank emphasised that virtual currencies are a form of unregulated digital money that can be used as a means of payment, noting that they do not have legal tender status in Ireland, and are not guaranteed or regulated by the Central Bank. 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 cited above.

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 the 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.

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 blanket 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. This is an approach that Andrea Enria, the Chair of the European Banking Authority has recently described as a "regulate and restrict approach".*

> *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".*"[4]

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 EU supervisory authorities.

On 24 September 2020, the European Commission adopted the Digital Finance Package. The Digital Finance Package includes 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. The MiCA will replace existing national frameworks applicable to crypto-assets not covered by existing EU financial services legislation. It will establish uniform rules for crypto-asset service providers and issuers at EU level, provide measures ensuring consumer and investor protection, and include safeguards to address potential risks to financial stability. In April 2021, Sharon Donnery, Deputy Governor, Central Banking at the Central Bank, stated that:

> "*... the Central Bank is supportive of the European Commission's work on advancing an EU framework for markets in crypto-assets and welcomes the development of a more harmonised approach to crypto-assets.*"[5]

However, until the 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.

The adoption of the Digital Finance Package follows the publication by the European Commission of a consultation paper on the future EU framework for markets in crypto-assets, on 19 December 2019. The consultation paper consists of three substantive parts, namely: (1) classification of crypto-assets; (2) crypto-assets that are not currently covered by EU legislation; and (3) crypto-assets that are currently covered by EU legislation. This consultation was the first step taken at EU level in preparing potential initiatives to specifically regulate crypto-assets in the EU.

In response to that consultation, the Central Bank issued a letter dated 30 April 2020 to the Directorate-General for Financial Stability, Financial Services and Capital Markets Union of the European Commission, in which the Central Bank advised that it is supportive of the initiative and that it welcomes the development of a more harmonised approach to crypto-assets. The Central Bank expressed the view that a harmonised taxonomy at EU level would facilitate a feature-driven, case-by-case assessment by market participants and, as appropriate, National Competent Authorities, given the evolving nature of crypto-assets.

"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*".[6] However, an exception to this may apply in relation to the category of cryptocurrencies known as "*stablecoins*" – particularly, where these are pegged to, and are directly exchangeable on demand for, fiat currencies.

In the 2019 consultation, the European Commission sought to determine whether additional regulatory requirements should be imposed on both "stablecoin" and "global stablecoin" issuers when their coins are backed by real assets or funds. 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 a transferable security for the purposes of MiFID.

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*".[7]

Key to any future regulation of security tokens at an EU or Irish level will be the concepts of "financial instrument" 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 well 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 will need to be authorised as an investment firm (and will need to comply with a wide range of detailed prudential and conduct of business requirements) unless it benefits from an exemption.

The European Commission's Digital Finance Package introduces a draft Directive, which, in addition to clarifying certain provisions in existing EU financial services directives, amends the definition of a "financial instrument" in MiFID to clarify beyond any legal doubt that such instruments can be issued via DLT.[8]

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 subsequently updated in April 2020).

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. Cryptocurrency is treated the same as any other foreign currency and as cryptocurrencies are not a functional currency for tax purposes, a company's accounts cannot be prepared in cryptocurrencies for tax purposes.

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 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 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.

While cryptocurrencies are treated in the same manner as any other foreign currency, 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. Although the Court of Justice of the European Union and the Irish Revenue have adopted a different basis on which the actual transfer of cryptocurrencies are VAT-exempt, they nevertheless have ultimately come to the same result. 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 may be of significance in determining whether a person is subject to Irish tax (in particular non-Irish residents) in cross-border dealings. This is an area that is likely to evolve over time.

Money transmission laws and anti-money laundering requirements

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 appears relevant in the case of classic cryptocurrencies, 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 could be viewed as being engaged in the regulated activity of money remittance/transmission.

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 European Banking Authority (**EBA**) has indicated that, in certain circumstances, a crypto-asset could qualify as "electronic money",[9] 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.

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 "virtual asset service providers" (**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*".

VASPs are now 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 2021, Derville Rowland, Director General, Financial Conduct at the Central Bank, stated in reference to VASPs that:

> "*The Bank has developed a registration and supervisory framework for this cohort of firms. In 2021, we will focus on assessing the AML/CFT frameworks of these firms to ensure that they are minimising their ML/TF risk.*"[10]

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 European Commission's Digital Finance Package introduces a draft Regulation, which establishes a pilot regime to allow regulators to gain experience of the use of DLT in market infrastructures and to allow companies to test out solutions using DLT.[11] The pilot regime provides for derogations from existing rules and 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, with such restrictions most likely excluding crypto-assets. However, there are no generally applicable restrictions in Ireland on investment managers holding crypto-assets for investment purposes, and as such, the regulatory position is unclear.

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.[12] 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. "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.
5. "The Future of Payments in Ireland and Europe" – opening remarks given by Sharon Donnery, Deputy Governor, Central Banking, Central Bank of Ireland on 28 April 2021.
6. https://www.centralbank.ie/consumer-hub/consumer-notices/consumer-warning-on-virtual-currencies (updated April 2021).
7. Speech at Digital Finance in Europe by Gerry Cross, Director of Financial Regulation – Policy and Risk, Central Bank of Ireland on 14 May 2020.
8. Proposal for a Directive of the European Parliament and of the Council amending Directives 2006/43/EC, 2009/65/EC, 2009/138/EU, 2011/61/EU, EU/2013/36, 2014/65/EU, (EU) 2015/2366 and EU/2016/2341.
9. See Box 3 on page 13 of the EBA's Report on Crypto Assets.
10. "Conduct, culture and trust – priorities for 2021" – speech given by Derville Rowland, Director General, Financial Conduct, Central Bank of Ireland on 16 March 2021.
11. Proposal for a Regulation of the European Parliament and of the Council on a pilot regime for market infrastructures based on distributed ledger technology.
12. 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 and e-money firms, 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 payments and e-money sector and he is currently advising a leading international crypto-assets and payments firm on their application 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 and Chief Compliance Officer of a regulated 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

Italy

Massimo Donna & Chiara Bianchi
Paradigma – Law & Strategy

Government attitude and definition

Boosting the adoption of digital technologies has been a priority for Italy's government over the past few years. In fact, 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 in general, and specifically its application in the field of cryptocurrencies, has been the centrepiece of the latest government's efforts to promote innovation. Such efforts, however, have been partially stymied by a general resistance to adopt new payment systems in a country where cash is still the most common way to settle bills, which of course might facilitate tax evasion.

This resistance led the government to press ahead with its plan to turn Italy into a cashless society, by passing a law granting significant rebates to taxpayers who avoid paying in cash. Whilst such a measure is primarily aimed at fighting tax evasion, it will very likely make alternative payment methods, including cryptocurrencies, more popular with the general public. Such government programme, dubbed "Cash Back", has now been called into question as critiques say it has not delivered on its promises to reduce tax evasion, but political pressure is mounting to keep it in force. A further boost towards cashless payment has of course been prompted by the COVID-19 crisis, during which cash was seen as a potential means of infection and online purchases warranted digital payment.

Italy has also passed legislation aimed at introducing a statutory definition of blockchain and smart contracts. In fact, by way of Law Decree no. 135/2019, distributed ledger technologies ("**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.*" Of course, 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 2019 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. Smart contracts

meet the written requisite, as required under Italian law in certain circumstances, by way of digital identification of the interested parties as per certain guidelines to be issued by *Agenzia per l'Italia Digitale*, a government agency charged with overseeing and promoting the adoption of innovative digital technology in Italy. In general, the coronavirus pandemic forced Italian small and mid-size businesses to embrace e-commerce and digital innovation, with many commentators forecasting new blockchain use cases.

The Italian legal system does not include a general definition of cryptocurrencies (although, as we will analyse later, sector-specific definitions have been introduced). 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 (http://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 very 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 European Central Bank.

Cryptocurrency regulation

Although, as mentioned above, 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

transposed in Italy the Fourth Anti-Money Laundering Directive, 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.*" This is certainly just an initial attempt to define such a complex phenomenon as cryptocurrencies and one in which virtual currencies are defined broadly, as the aim of the statute including the definition was to capture the wider possible range of digital assets to prevent them from being used for money laundering and to facilitate terrorism.

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 and damaging third parties may be sentenced to imprisonment for up to six years as well as to a fine of up to EUR 3,000. The above-mentioned maximum imprisonment and financial sanctions 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

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 cryptocurrencies 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 Capital Markets Code (*Testo Unico della Finanza*, or "**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 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 crypto assets are offered to Italian customers; 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 appears to have taken a harder stance, claiming that an offer was directed to Italian customers simply because the website owner had not taken any active measure to prevent Italian customers from accepting the offer. In this context, however, the Italian Supreme Court (ruling no. 26897 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.

The above being the general landscape, over the past few years, CONSOB has on several occasions sanctioned initial coin offerings ("**ICOs**") for breaching Italian law.

In fact, CONSOB has pointed out that, depending on the characteristic of the relevant crypto assets, they may or may not fall within the definition of Financial Products. Indeed, whilst *payment tokens* are typically not Financial Products and *security tokens* are, so-called *utility tokens* constitute a grey area that needs to be assessed on a case-by-case basis. For example, utility tokens often seem to only entitle the token-holder to receive a product or service in the future, but the token-holder may also intend the purchase of the token as an investment, hoping, in fact, that the future services or goods will appreciate over time, consequently causing an appreciation of the underlying "utility" token. In such a case, what at first may seem a utility token, on further analysis may reveal itself to be an investment token. Equally, some payment tokens may be purchased as a speculative investment instrument in light of their high volatility.

However, CONSOB soon realised that regulating ICOs in such a way based on an *ad hoc* analysis of the characteristics of the tokens to be issued does not guarantee the level of legal and regulatory certainty that is necessary to promote ICOs as a mainstream way to fund new entrepreneurial initiatives.

Furthermore, in 2019, CONSOB launched a public consultation on ICO regulation in Italy. In the consultation, CONSOB depicted a draft ICO regulation to be applied to crypto assets that fall within the definition of Financial Products under the TUF with the exclusion of those assets that, as Financial Instruments, fall within the field of application of MiFID II and therefore cannot be regulated on a national basis. According to the draft project, crypto asset issuers may opt to offer crypto assets through authorised platforms, which, at least initially, may coincide with those offering equity crowdfunding services under the relevant CONSOB regulation. The idea was to incentivise promoters to launch ICOs through *ad hoc* "platforms for the offer of crypto assets" by exempting them from the prospectus and distance offering rules. At the same time, customers would be more willing to purchase crypto assets

offered through such CONSOB-regulated platforms. In January 2020, CONSOB published the comments received – mostly from financial institutions, universities and law firms – which covered a number of issues, from the definitions of DLT and blockchain that in the consultation document appeared to coincide, to the security measures that ICO platform managers should adopt. COVID-19 has generally slowed down the government's action outside the urgent measures to weather the pandemic, and CONSOB has not yet followed through on its plan to regulate ICOs.

Taxation

Cryptocurrency taxation is still unregulated in Italy. In fact, the Italian tax authority (*Agenzia delle Entrate*) has been trying to address the taxation of crypto assets by regarding them as falling within the definition of other, more traditional assets and applying the relevant tax regimes.

(i) **VAT**. When dealing with the VAT regime of cryptocurrencies, the Italian tax authorities have relied on the Court of Justice of the European Union's ("**CJEU**") finding in *Skatteverket v David Hedqvist* Case C-264/14. In such a ruling, the CJEU stated that cryptocurrencies may be treated as foreign currencies for VAT purposes, and therefore the exchange of cryptocurrencies should be exempted from VAT pursuant to article 135, para 1, letter e) of EC Directive 112/2006 (the "**VAT Directive**"). Consequently, in its Deliberation no. 72/E of 2016, the *Agenzia delle Entrate* confirmed that the exchange of cryptocurrencies is exempted from VAT under the applicable Italian legislation transposing the VAT Directive in Italy.

(ii) **Corporate taxation**. The Italian tax authorities have stated that the profits deriving from cryptocurrency trading are relevant for the purposes of corporate income tax (IRES and IRAP) and must be included in the company's financial statements.

(iii) **Personal income tax**. The profits generated by non-professional crypto asset trading are regarded as those deriving from forex trading for personal tax purposes, and capital gains taxation will only apply to such profits if the relevant individual has held on his/her accounts more than EUR 51,645.69 worth of cryptocurrency (at the applicable exchange rate on 1 January each year). In their annual tax return, individuals residing in Italy must specify whether they have any cryptocurrencies held in e-wallets, just as they have to declare if they have money held in foreign bank accounts.

Money transmission laws and anti-money laundering requirements

EU Directive 2016/0208 (the "**AML 5 Directive**") has been 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 Register of Financial Agents and Credit Mediators. 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 *vice versa*, whilst under the new rules also applies 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 is, 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 transactions 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.).

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, for a period of 10 years.

Finally, Crypto Service Providers must report suspicious transactions to the competent authorities.

Promotion and testing

A long-awaited piece of legislation introducing regulatory sandboxes for Fintech businesses was recently passed. In fact, on 2 July 2021, the Decree of the Ministry of Economy and Finance no. 100 of 30 April 2021 was published on the Italian Official Legal Bulletin and entered into force on 17 July 2021 (the "**Sandbox Decree**"). Whilst the Sandbox Decree is aimed at fostering all types of Fintech innovation, blockchain will likely play a prominent role in the sandbox experiment.

The idea behind the Sandbox Decree is to set up a Fintech Committee composed of representatives of all the authorities potentially involved in the authorisation or supervision of Fintech businesses, i.e. the Italian Financial Markets Watchdog (CONSOB), the communications authority (AGCOM), the competition authority (AGCM), the data protection authority, the governmental body in charge of digitalisation, the tax agency, and the insurance watchdog. The working of the Fintech Committee is described in detail in an effort to establish a comprehensive but efficient process to evaluate sandbox applicants. Sandbox rights, if granted, last 18 months and, in certain circumstances, can be extended.

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, where her practice focuses on contentious commercial and IT matters.

Paradigma – Law & Strategy

Piazza Luigi Vittorio Bertarelli 1, 20122 Milan, Italy
Tel: +39 02 3655 2788 / URL: www.paradigma-law.com

Japan

Takeshi Nagase, Tomoyuki Tanaka & Takato Fukui
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**").

On the other hand, 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**").

In addition, tokens that constitute so-called "stablecoins" (i.e., tokens the prices of which are pegged to the value of fiat currency) will likely be classified either as Crypto Assets or a means of payment in fund remittance transactions (*kawasetorihiki*), depending on whether such stablecoins are redeemable in fiat currency.

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.

Recent developments

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.

However, as the legal status of NFTs is still unclear, significant legal issues will likely arise in the event of unforeseen circumstances, such as the hacking of NFTs or disputes over the rights of authors and purchasers of NFTs.

Central bank's attitude 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, in April 2021, the BOJ began exploring the technical feasibility of a general-use CBDC. In parallel with this, the BOJ also plans to study the institutional design aspects of CBDCs.

In addition, in July 2021, the Japan Financial Services Agency (the "**FSA**") established the Digital and Decentralized Finance Planning Office, which is expected to examine the laws and regulations specific to fiat-backed stablecoins.

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 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; 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.

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 (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 FSA Administration Guidelines on Crypto Assets 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 handling 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 with a new Crypto Asset to first conduct an internal assessment of the new Crypto Asset and submit an assessment report to the JVCEA. 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.

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 300 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, the Crypto Asset regulation under the PSA will apply. In accordance with current practice, (i) if the tokens issued via ICO are already dealt with by Japanese or foreign exchanges, such tokens would be considered to 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) even if certain tokens are not yet dealt with by Japanese or foreign exchanges, in a case where the token issuer does not give substantial restrictions prohibiting such tokens from being exchanged with Japanese or foreign fiat currencies or Crypto Assets, such tokens would likely fall within the definition of Crypto Asset under the PSA. Recently, in July 2021, Coincheck Inc., a CAESP registered under the PSA, started an initial exchange offering ("**IEO**") of the Palette Token (PLT). This is the first authorised IEO in Japan.

In addition, the JVCEA has published self-regulatory rules and guidelines regarding ICOs for Crypto Asset-type tokens, entitled "Rules for Selling New Crypto Assets" (the "**ICO**

Rules"). According to the ICO Rules, there are two types of ICO, which can be described as follows: (i) an Exchange Provider issues new tokens and sells such tokens by itself; or (ii) 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" (*maebarai-shiki-shiharai-shudan*), 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.

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.

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 regulation 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.

An Exchange Provider 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 FSA, 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.

Tomoyuki Tanaka
Tel: +81 3 6775 1218 / Email: tomoyuki.tanaka@amt-law.com

Tomoyuki Tanaka is a partner specialising in financial regulatory issues, financing transactions and corporate transactions. He has considerable experience advising on all aspects of financial regulatory issues, including fintech-related matters. He has served on secondment in the supervisory department of the FSA, where he had regulatory oversight of various financial institutions, such as banks, securities companies and fintech companies.

Takato Fukui
Tel: +81 3 6775 1207 / Email: takato.fukui@amt-law.com

Takato Fukui advises fintech companies, financial institutions and self-regulatory organisations on a broad range of legal issues, including Crypto Asset-related matters. From 2014 to 2017, he worked at the FSA, where he oversaw operators of fund remittance transactions and prepaid card issuers regulated under the PSA, as well as money lenders under the Money Lending Business Act. At the FSA, he was also instrumental in preparing the FSA Guidelines for Virtual Currencies Exchange Business Operators. From 2018 to 2020, he served as Director General of the JVCEA, where he was significantly involved in developing a set of self-regulatory rules and obtaining FSA certification for the JVCEA as a self-regulatory organisation registered under the PSA and FIEA.

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

Jersey

Christopher Griffin, Emma German & Holly Brown
Carey Olsen Jersey LLP

Government attitude and definition

Jersey continues to welcome fintech including cryptocurrencies, blockchain and distributed ledger technology ("**DLT**") more widely as a pioneer in fintech regulation. Jersey enjoys a sophisticated legal, regulatory and technological infrastructure, supporting development and innovation in fintech, including:

- payment services and online payment solutions;
- electronic identification ("**E-ID**");
- virtual currency exchanges ("**VCEs**") (cryptocurrency exchanges);
- security token and non-security token issuances and initial coin offerings/security token offerings ("**ICOs**"/"**STOs**");[1]
- custody services and arrangements for holding digital assets; and
- fintech funds and other vehicles.[2]

Jersey is fast becoming an established market for fintechs and professional investment firms, being home to a number of token issuers, global payment platforms and fintech-focused investment funds. In the past few months alone, Jersey has seen multimillion-pound investments and capital raises structured using Jersey vehicles and advisers. Jersey clients include tech giants, cryptocurrency exchanges, payment platforms and emerging blockchain developer talent.

Jersey recognised cryptocurrencies as a separate asset class long before the "ICO Craze" of 2017, when the Island's regulator, the Jersey Financial Services Commission (the "**JFSC**"), licensed the world's first Bitcoin-focused, regulated fund (GABI Plc). From that point onwards, the Island has seen a surge in exchange vehicles, token issuers and fintech funds choosing Jersey, including the world's largest investment fund (the SoftBank "Vision Fund", which raised USD 97 billion over two years). Both GABI and SoftBank were advised by Carey Olsen.

The JFSC is a member of the Global Financial Innovation Network and participates in the cross-border testing pilot.

Jersey has an exceptional pool of blockchain expertise, developed from the JFSC's forward-thinking attitude combined with Jersey's flexible range of corporate vehicles and favourable tax regime.

Examples of structures that have recently used Jersey (advised in each case by Carey Olsen) include:

- CoinShares (Europe's largest digital asset investment firm with USD 3 billion in assets under management ("**AUM**")) recently used Jersey for the establishment of its new institutional-grade cryptocurrency-backed exchange-traded product ("**ETP**").

CoinShares Physical Bitcoin (Ticker: BITC) launched on 19 January 2021 with USD 200 million in AUM, and is the first CoinShares product to be listed on the SIX Swiss Exchange. The ETP programme's physically backed structure provides institutions that are experienced in trading similar commodity-based investment securities with a familiar structure for cryptocurrency investments.

- CoinShares previously used Jersey for the launch of its ETH denominated investment fund (2017), which provided investors with exposure to the liquid digital asset ecosystem, and the 2014 launch of the first-ever regulator-approved Bitcoin investment fund.
- Radix, a decentralised finance platform, used Jersey for the launch of its utility token. The platform allows users to transact with each other over a fast, secure blockchain-based platform without the need for intermediaries. Tokenholders are able to use the tokens to pay transaction fees and/or to participate in the platform's "proof of stake" consensus mechanism to validate transactions.
- Global payment solutions provider Checkout.com, which undertook a USD 450 million Series C fundraising round. The transaction gave the company a post-money valuation of USD 15 billion, making Checkout.com the fourth-largest fintech globally and the EMEA's most valuable venture-backed business.
- Token issuer PIP Limited used Jersey for the launch of its Vow token ecosystem, a solution for distributing debt-free liquidity into local communities through a customer loyalty mechanic.

Jersey distinguishes between traditional fiat currency and cryptocurrencies and does not treat cryptocurrencies on an equal footing to fiat currencies. For example, regulations around holding client monies focus only on fiat. Within cryptocurrencies, Jersey distinguishes between utility tokens and security tokens, as set out in the ICO guidance published by the JFSC.

There are no cryptocurrencies backed by the Government of Jersey and Jersey does not have a central bank. Jersey uses British pound sterling, although the States of Jersey Treasury issues its own bank notes separate to those in the UK.

In terms of trends, we are seeing an increased use of, and enquiries relating to, funds rolling out crypto-backed products, primarily but not limited to Bitcoin- and Ethereum-backed products, online payment solutions and E-ID and a continued interest in the establishment of cryptocurrency and security token exchanges. More recently, as a result of COVID-19, we are seeing a sharp increase in the uptake of technology and new entrants to the market. Whilst not fintech as such, this includes a widespread use and adoption of electronic signatures (including witnessing) and a general shift towards digitisation and automation of manual procedures consistent with a widespread move to remote working. We are therefore expecting this trend to continue in the coming months and welcome the opportunities that this may present in terms of increased usage of blockchain and smart contracts and automation and AI in Jersey.

In terms of innovation generally, Jersey is striving to promote fintech development by supporting local fintech talent and innovation. Digital Jersey, a Government-backed economic development agency and industry association dedicated to the growth of the digital sector, aims to do this. Further, the JFSC is a member of the Global Financial Innovation Network and participates in the cross-border testing pilot. COVID-19 has also brought about pragmatic developments in Jersey's legal practice and has given rise to recent guidance from The Law Society of Jersey in relation to the signing of certain powers of attorney by electronic signature, which demonstrates Jersey's willingness to adopt technological developments.

Blockchain and cryptocurrency/digital asset regulation

To date, Jersey has not sought to introduce any fintech-specific legislation. The JFSC has sought to cater for fintech businesses within the existing regulatory framework until such time as there is a global consensus on how to regulate aspects of the fintech ecosystem; for example, if the fintech service involves the provision of a financial service, it will fall to be regulated within Jersey's financial services regime under the Financial Services (Jersey) Law 1998 (the "**FSJL**") unless an applicable exemption is available. The FSJL defines "financial services business" as investment business, trust company business, general insurance mediation, money services business, fund services business or alternative investment fund services business.

The main types of fintech activities that are currently active in Jersey and require some level of regulatory oversight are:

- **Payment services** – depending on the payment services being offered, these may be required to be regulated under the FSJL to undertake "money services business", trust company business (as outlined above to the extent the services include an e-wallet relating to digital assets) or under the Banking Business (Jersey) Law 1991 for "deposit-taking" business. There are a number of exemptions that may apply and early advice should be sought.
- **VCEs** – these exchanges must maintain a registration under the Proceeds of Crime (Jersey) Law 1999 (the "**POCJL**") as a "supervised business". The POCJL requires VCEs to comply with Jersey's laws, regulations, policies and procedures aimed at preventing and detecting money laundering and terrorist financing.
- **Security token exchanges** – these exchanges are currently required to be regulated under the FSJL to undertake "investment business" (an "**IB Licence**"). A standard application for an IB Licence will take approximately eight weeks. An application for a digital assets-related matter may take a little longer. A full regulatory application to the JFSC will be required and will include the following documents:
  (a) a regulatory application form;
  (b) a business plan; and
  (c) a business risk assessment.

  In terms of regulatory capital requirements, the main requirement to be aware of is that an exchange platform will be required to maintain at all times:
  (a) a net liquid assets position of 130% of its projected quarterly expenditure;
  (b) a minimum of GBP 25,000 paid-up share capital; and
  (c) a minimum net assets position of GBP 25,000.

  In addition, a Jersey security token exchange must be audited and the composition of the board must comply with the Jersey regulatory and economic substance requirements, being:
  (a) there must be a minimum of two Jersey resident directors;
  (b) the board must meet with adequate frequency having regard to the amount of decision making being undertaken;
  (c) at meetings there must be a quorum of directors physically present in Jersey; and
  (d) the directors of the company must have the necessary knowledge and expertise to discharge their duties (this is assessed on a whole-board basis).

  Once an IB Licence has been obtained, the holder will need to observe the provisions of the JFSC's Code of Practice for Investment Business:
  - There are locally regulated administrators in Jersey who can assist by providing "incubation" services to entities and groups that are new to Jersey.

- There is no requirement to have electronic clearing and settlement or for clearing of security tokens to be carried out by a clearing house or central depositary.
- The increase in uptake of exchange-related investment business in Jersey has resulted in the JFSC consulting on proposed amendments to the class of investment business to include a specific new category of exchange business. We await the outcome of the Consultation.

- **Custody services and arrangements for holding digital assets** – there are two models: (i) custody services provided by the exchange itself (or a related entity) to investors and exchange users; and (ii) custody services outsourced to a third-party custody provider to be provided to investors and exchange users.
  In both models, where digital assets will be stored offline or where the investor or exchange user is not provided with the keys to access the digital asset, the investor/exchange user will no longer have control over the digital assets they have invested in. In this way, it is likely that the relevant custodian entity will be providing trustee services and will need to be regulated for "trust company business" under the FSJL. However, where the storage of digital assets is incidental or ancillary to the main purpose of the entity and where there was no separate remuneration, an exemption may apply. Early advice should be sought on this point, and this is something Carey Olsen has experience of advising on.
- **Business relating to digital assets and cryptocurrency** – the JFSC will treat involvement by Jersey structures with digital assets and cryptocurrencies as a "sensitive activity" under the JFSC's Sound Business Practice Policy. The practical consequence of this is that certain anti-money laundering/countering the financing of terrorism ("**AML/CFT**") obligations are imposed on the Jersey structure. For instance, a token-issuing company is required to carry out checks on: (i) the purchasers of the tokens who purchase coins directly from the issuer; and (ii) the holders of tokens issued by the issuer in the event they are sold back to the issuer. In such circumstances, the issuer will be required to obtain information to: (a) establish and obtain evidence to verify identity; and (b) establish and, depending on the level of risk, obtain evidence to verify the source of funds and source of wealth.

Sales regulation

In Jersey, the sale of Bitcoin or other crypto or digital tokens *per se* is not regulated by a specific securities law or commodities law. As noted above, transactions relating to digital assets and cryptocurrencies are treated as a "sensitive activity" under the JFSC's Sound Business Practice Policy. In addition, there are requirements under Jersey's existing regulatory framework for sale transactions that arise in the following circumstances:

- token issuers (whether utility tokens or security tokens) who issue or offer tokens for sale;
- companies operating VCEs – these exchange fiat monies to cryptocurrencies and *vice versa*; and
- companies operating security token exchanges – these exchange fiat monies to security tokens and *vice versa*.

The sale of cryptocurrencies in the secondary market (such as on an exchange) in return for payment in cryptocurrencies (i.e. crypto-to-crypto transactions) does not fall within the VCE or security token exchange regime although would still be considered a "sensitive activity" as outlined above.

Taxation

Jersey provides a stable, tax-neutral environment. Many Jersey companies (apart from locally regulated financial services companies and utilities) can be zero-rated for income tax and are not subject to capital gains tax within the jurisdiction. Jersey has no capital transfer or similar taxes and does not levy any withholding tax on dividends. There is also no stamp duty on Jersey share transfers. Companies can also be incorporated in Jersey but can be resident for tax purposes in another jurisdiction if certain criteria are met.

There are currently no specific laws regulating the taxation of cryptocurrencies or digital assets, although Jersey's Comptroller of Taxes has issued guidance on cryptocurrency tax treatment regarding both Jersey income tax and Jersey goods and services tax. The guidance provides that such assets will be taxed in accordance with general Jersey taxation principles and provisions.

Money transmission laws and anti-money laundering requirements

In terms of money transmission, as noted above, depending on the services in question, payment services business and money transmission services may be required to be regulated under the FSJL in order to undertake "money services business", trust company business (as outlined above to the extent the services include an e-wallet relating to digital assets) or under the Banking Business (Jersey) Law 1991 for "deposit-taking" business. There are a number of exemptions that may apply and early advice should be sought.

In terms of AML, as noted above, the JFSC will treat transactions with digital assets and cryptocurrencies as a "sensitive activity" under the JFSC's Sound Business Practice Policy. The practical consequence of this is that certain AML/CFT obligations are imposed on the issuer from Jersey's AML regime. This includes the issuer being obliged to carry out checks on: (i) the purchasers of the tokens who purchase coins directly from the issuer; and (ii) the holders of tokens issued by the issuer in the event they are sold back to the issuer. In such circumstances, the issuer will be required to obtain information to: (a) establish and obtain evidence to verify identity; and (b) establish and, depending on the level of risk, obtain evidence to verify the source of funds and source of wealth.

In addition, Jersey also has an industry working group focused on managing Virtual Assets Risk in relation to Virtual Assets and Virtual Assets Service Providers ("**VASPs**"). This working group involves Carey Olsen representatives, the Government of Jersey representatives, JFSC representatives and other interest groups on the Island. The working group is reviewing the Island's AML requirements in relation to Virtual Assets and VASPs.

Promotion and testing

Jersey promotes and tests fintech firms' products and services in a number of ways.

In terms of testing products and services, the JFSC has proven itself to be a proactive and forward-thinking regulator in becoming a member of the Global Financial Innovation Network (a group of international regulators and observers committed to supporting innovative products and services) and participating in the cross-border testing pilot that launched in January 2019, offering firms the opportunity to test their products and services in multiple jurisdictions.[3]

Jersey also operates a sandbox run through Digital Jersey, supporting local fintech firms and fintech firms seeking to relocate to Jersey.[4]

In terms of promoting fintech and thought-leading in Jersey, the Digital Assets Working Group (the "**DAWG**") works hard to raise awareness and interest in Jersey. Combining representatives of the States of Jersey, representatives of the JFSC and other interest groups on the Island, the DAWG is a group of individuals knowledgeable in the fintech space promoting digital assets and blockchain technologies in Jersey. Carey Olsen is a founder member of the DAWG and is an active participant and contributor.

Ownership and licensing requirements

There are no specific additional restrictions or licensing requirements on investment managers owning cryptocurrencies for investment purposes or holding cryptocurrency as an investment advisor or fund manager. We are seeing many fund structures starting to invest in cryptocurrencies and offering crypto-related products. The usual rules applicable to investment managers continue to apply in terms of both the general regulations applicable to them to undertake investment business and in relation to the investment policies described in their offer documentation.

However, as noted above, cryptocurrency-related transactions do constitute "sensitive activities" and we would expect to see additional business risk assessments, policies and procedures relating to that specific asset class. This includes a level of diligence on the providence of the cryptoasset in question to detect any prior illicit activity relating to the asset. There are various service providers such as Chainalysis and Merkle Science that carry out crypto threat detection (i.e. previous transaction screening) and related services that can be used to mitigate the potential risk of acquiring tainted assets.

We do advise fund managers and investment managers looking to enter this space to make contact with us so that we can advise as appropriate. In some instances, it may be appropriate to address new policies with the JFSC.

Mining

Mining cryptocurrencies is not covered by any specific piece of legislation or regulation in Jersey. However, depending on the manner in which mining activities are conducted, it may fall within the existing regulatory framework for funds (mentioned above).

Border and declaration

At present, there are no border restrictions in place on declaring cryptocurrency holdings.

Reporting restrictions

Equally, there are currently no specific reporting requirements triggered for cryptocurrency payments.

Estate planning and testamentary succession

Cryptocurrencies are treated as intangible movable property. If the owner of the cryptocurrency is a natural person, then the cryptocurrency falls to be dealt with within the movable estate of the owner on his/her death. Although there is no decided case on the point, it is generally assumed that the Jersey Courts would determine the *situs* of any cryptocurrency by reference to Jersey's private international law rules, which broadly follow and adopt English private international law principles.

Additional considerations need to be given to the practicalities of accessing the digital assets and ensuring that the testator shares access to all private keys, hot and cold wallets

and any other form of password-protected account with the administrator or executor of his/her estate to ensure that the digital assets are capable of being accessed and transferred in accordance with the testator's will in the event of his/her demise.

The future of DLT in Jersey

As a nascent technology, international industry practices around blockchain and DLT are still evolving and their applications and use cases (including outside the finance industry) being asserted. To maintain its place as a respected, well-regulated international finance centre, Jersey is cognisant, and encouraging, of the advantages blockchain and DLT bring to Jersey's finance industry.[5]

As a long-established, well-regulated international finance centre, Jersey boasts a host of industry experience and local expertise,[6] making it an ideal jurisdiction to launch new blockchain and DLT initiatives.

Leveraging this existing expertise and the low-tax environment, we expect to see Jersey and Jersey vehicles continue to be used in both established areas of finance as they embrace blockchain solutions (such as climatech, proptech, online settlement solutions, E-ID and regtech, etc.) and new areas of finance and other sectors as blockchain and DLT use cases are established.

The JFSC's considered and measured approach to fintech regulation to date should equip Jersey to be a leading blockchain and DLT jurisdiction of the future by ensuring that regulation in Jersey remains appropriate and commensurate to the product or service in question.

We would be happy to discuss any blockchain or DLT initiatives backed by persons of substance. Please do contact us using the details below.

* * *

Endnotes

1. In the fintech space, the ICO terminology has now largely been superseded by reference to security and non-security tokens, a reflection of the evolving regulatory backdrop. We retain reference to ICOs in this chapter because we, Carey Olsen, have advised in relation to a number of ICOs and that was the terminology used at that time. The settled approach now is to determine whether a coin or token or other digital asset issued constitutes a security or not and therefore whether it is a "security token" or not. We have addressed STOs and non-security token issuances separately.
2. There is JFSC guidance available at: https://www.jerseyfsc.org/media/2003/2018-07-12_jfsc-issues-ico-guidance-note.pdf. It has been confirmed that this JFSC guidance has a wider application and can be used to inform how digital assets and cryptocurrencies more generally will be treated.
3. The window for applications to participate in the January 2019 pilot has now closed.
4. *See*: https://www.digital.je.
5. Such as: (i) real-time settlement; and (ii) greater transparency as to origination or provenance of the asset in question. For example, as Jersey currently has no restrictions or requirements around financial settlement, Jersey is an ideal jurisdiction from which to launch securities and cryptocurrency exchanges.
6. Including in banking, international payments, compliance, funds, capital markets, real estate and company administration.

Christopher Griffin
Tel: +44 1534 822 256 / Email: christopher.griffin@careyolsen.com

Christopher spearheads Carey Olsen's crypto practice and digital assets team, advising on the launch in 2017 of CoinShares Fund I (a venture cap fund investing in crypto assets) and ARC Reserve Currency, Jersey's first initial coin offering or "ICO". Christopher was instrumental in the launch of the Jersey platform for Binance, the world's largest cryptocurrency exchange. Christopher also advises on all aspects of fund and corporate transactions, including the legal and regulatory aspects of fund launches, and joint ventures. He also has considerable experience in dealing with the Jersey Financial Services Commission in navigating investment vehicles through the Jersey regulatory approval process.

Christopher has broad experience of both general international corporate and funds work with particular expertise in private equity and hedge funds, having spent 10 years as a corporate and funds lawyer in the City.

Emma German
Tel: +44 1534 822 474 / Email: emma.german@careyolsen.com

Emma is a senior associate in the Carey Olsen Jersey digital assets team and has advised in relation to a number of blockchain and digital asset-related matters, including in relation to: payments, the establishment of virtual currency exchanges and security token exchanges; the use of Jersey vehicles for token issuances; and digital company administration in Jersey.

Emma is a Jersey Law Commissioner and actively involved in efforts to reform Jersey law to support fintech and innovation and has published a paper on the recognition of smart contacts.

Emma has a background in international corporate and finance transactions and her expertise includes the raising of finance through the issuance and listing of Eurobonds and other securities on The International Stock Exchange. Emma is an advocate of the Royal Court of Jersey. She is a barrister of England and Wales (non-practising) and an English solicitor. She was educated at King's College London. Emma joined Carey Olsen in 2005.

Holly Brown
Tel: +44 1534 822 231 / Email: holly.brown@careyolsen.com

Holly is an associate in Carey Olsen's Jersey corporate department. She is a member of the digital assets team and has assisted with various matters related to cryptocurrencies/digital assets and blockchain, including the launch of Binance's Jersey exchange platform and in relation to payments. Holly also advises on the raising of finance by issuers and the listing of Eurobonds and other securities on The International Stock Exchange, having completed a secondment to The International Stock Exchange.

Holly is an advocate of the Royal Court of Jersey. She was educated at King's College London. Holly joined Carey Olsen in 2013.

Carey Olsen Jersey LLP

47 Esplanade, St Helier, Jersey JE1 0BD, Channel Islands
Tel: +44 1534 888 900 / Fax: +44 1534 887 744 / URL: www.careyolsen.com

Kenya

Muthoni Njogu
Njogu & Associates Advocates

Introduction

The crypto economy worldwide has experienced significant milestones, fuelling the record surge of the digital asset, and the industry is expected to maintain momentum despite the fluctuations in its value. The first and second quarters of 2021 were punctuated by noteworthy developments in the field of cryptocurrencies, wherein the crypto market not only attracted retail investors, but also traditional financial institutions and large corporations that are looking to profit from the emerging trend of digital assets. The world is experiencing the greatest appreciation of cryptocurrency in history, and it is becoming clear that this will not be going away anytime soon.

Africa is no exception, and Kenya is one of the three largest Bitcoin markets in Africa alongside giants like Nigeria and South Africa. Kenya recorded an increased trading volume of cryptocurrencies on "peer-to-peer" (P2P) transactions. This was aptly captured by firms like LocalBitcoins, a P2P Bitcoin marketplace that facilitates over-the-counter trading of local currency for Bitcoins. As at Q2 2021, statistics from LocalBitcoins revealed that Bitcoin usage has skyrocketed, with volumes of more than $920,000 being traded on the platform each week. The most popular payment methods being: mobile banking; internet banking; ATMs; agencies; branch to the tune of $10,000; and interestingly, through PesaLink, which enables one to transfer funds from one bank account to another in real time through the various bank channels. The Head of Business Development of LocalBitcoins stated that:

> "*The record trading volume in Kenya was achieved during the second week of January 2021 when as much as KES 150 million worth of bitcoin was traded on our platform, which amounts to $1.3 million. $1.3 million puts Kenya in the top echelon of the countries on LocalBitcoins by trading volume. Only a handful of countries have ever broken that $1 million a week barrier.*"[1]

To sweeten the pot, the platform began to offer zero deposit fees for all incoming transactions to users' wallets and we can therefore expect the numbers to grow exponentially.[2]

In addition, Chainalysis, the blockchain data platform offering crypto analysis, among other things, offered insights into the emerging markets, including Kenya. In its report, it revealed that Kenya is now ranked as leading adopter of cryptocurrency, sitting at position five in the world on global cryptocurrency activity. Chainalysis indexed the outcome on three pertinent pillars, namely: on-chain cryptocurrency value received, which captures all total crypto activity; on-chain retail value transferred, which measures how much cryptocurrency individuals are transacting; and P2P trading volumes.[3]

It is evident that based on the above-captured metrics and numerous others carried out in previous years, Kenya has witnessed huge transaction volumes on P2P platforms

when adjusted for GDP *per capita* and the internet-using population. The report further highlighted that many residents use P2P cryptocurrency exchanges as their primary on-ramp into cryptocurrency, premised by the fact that they did not have access to centralised exchanges. The pertinent question to ask is why are Kenyans using these platforms? It goes without saying that Kenya is not estranged from the problems that bedevil Africa as a whole and from the report, it is clear that many turn to cryptocurrency to preserve their savings in the face of currency devaluation, send and receive remittances, and generally carry out business transactions.[4]

Aside from trading volumes, notable developments and projects in the blockchain and crypto space have witnessed an initial pilot testing of the usage of Akoin. The cryptocurrency project, developed by Senegalese-American singer Akon, has achieved success in Western Kenya's Mwale Medical and Technology City, setting the stage for a national rollout.

The project's pilot phase commenced in November 2020 and is anticipated to have $5 million worth of transactions per month with residents exchanging value using Akoin. Complete deployment is expected to commence in September 2021, and monthly transactions are expected to surge to $2 billion by 2022.[5]

The year also witnessed the acceleration of Sarafu, a community inclusion currency that recently transitioned into a cryptocurrency. Established in 2017, the Sarafu Network is a basic income programme that aims to empower and support vulnerable Kenyan households by creating a cushion in times of financial crisis by distributing income tokens. Sarafu works like vouchers, which can be exchanged for goods or services. Anyone with a Kenyan mobile phone is eligible, including feature phones. The Kenya Red Cross, the largest humanitarian organisation in Kenya in conjunction with the Danish Red Cross and Grassroots Economics, launched the Sarafu Network to distribute the blockchain-based Sarafu token to anyone in Kenya. The Kenya Red Cross society's move came after the impressive success of the pilot programme in 2020, which saw over 40,000 households and small businesses join the Network following the COVID-19 pandemic.[6]

However, the issue that remains is how the lack of a clear, agreeable, multi-stakeholder policy on how to govern such cryptocurrencies and cryptocurrency businesses has led to a deadlock that has left room for hidden markets, scams and fraud to thrive, while locking out safe, viable, formal businesses and products. The question for Kenyan policy makers is whether they have the courage to let cryptocurrency and innovation take place in an intelligently regulated fashion with broad economic benefit, or the irresolution to force it to happen elsewhere.

Government attitude and definition

The top key regulators in Kenya for digital assets are the Capital Markets Authority (CMA) and the Central Bank of Kenya (CBK).

The CMA

2021 heralded some critical developments under the CMA.

Draft Capital Markets (Investment Based Crowdfunding) Regulations, 2021

The Cabinet Secretary for the National Treasury and Planning, through the CMA, published the Draft Capital Markets (Investment Based Crowdfunding) Regulations, 2021.[7] We look back to 2018 when the CMA issued warnings to investors against taking part in initial coin offerings (ICOs), a form of crowdfunding, as they had not approved any ICOs. This was predicated on the case of *Wiseman Talent Ventures Ltd*.[8]

The draft CMA regulations on investment-based crowdfunding are meant to control the raising of finances through crowdfunding platforms and protect the investors using the platforms. The regulations are aimed at ensuring that crowdfunding platforms are operated by licensed persons only and that participation on the platforms only involves eligible issuers and investors.

Attention must be paid to the wording of the regulations, which includes some interesting definitions under Section 1 of the draft regulations, *inter alia*:

> "*"crowdfunding platform" means a website, internet based portal or application operated by a crowdfunding platform operator which facilitates crowdfunding;*
> *"investment-based crowdfunding" means the process of crowdfunding in exchange for shares, debt securities or any other investment instruments approved by the Authority.*"

Due to the broad wording of the regulations, it can be opined that crowdfunding through ICOs is definitely catered for, albeit not expressly captured. In any event, the CMA stamped its authority in the case of *Wiseman Talent Ventures Ltd v Capital Markets Authority* [2019] eKLR, which was also amplified by the court ruling of the Honourable Judge in the same case.[9]

The key highlights of the regulations include, *inter alia*:

a. Issuers – issuers eligible to raise funds through a crowdfunding platform are start-ups with a good operating track record and good corporate governance record, and micro or small enterprises incorporated in Kenya for a minimum of two years.
b. To break this down, according to the Micro and Small Enterprises Act, 2012, a micro enterprise is defined as a firm, trade, service, industry or business activity whose turnover does not exceed $4,587 annually, which employs less than 10 people, and whose total assets are to be determined by the Cabinet Secretary from time to time. A small enterprise, on the other hand, means a firm, trade, service, industry or business activity whose annual turnover ranges from $4,587 to $45,870, which employs 10 to 50 people, and whose total assets and financial investment are to be determined by the Cabinet Secretary from time to time. Within a 12-month period, an eligible issuer can offer a maximum aggregate amount of investment as follows: $900,000 for medium enterprises; $459,000 for small enterprises; and $46,000 for micro enterprises.
c. However, a crowdfunding platform operator may apply to the CMA for a no-objection letter whenever an issuer seeks to raise more than the set limit within 12 months. Issuers prohibited from raising funds through the crowdfunding platforms include public listed companies and their subsidiaries, entities with a poor governance record, entities that propose to use the funds raised to provide loans or invest in other entities, and any other such entity as may be specified by the CMA. We wait to see the complete metrics for this, as currently worded it leaves a lot of room for interpretation.
d. Investors – eligible investors for crowdfunding include sophisticated investors and/or individual retail investors subject to an investment limit as prescribed by the platform operator and up to a maximum of $920. Investment instruments allowed for the purpose of crowdfunding include shares, bonds and debentures and any other instruments as approved by the CMA.
e. Platform operators – anyone who operates or intends to operate a crowdfunding platform in Kenya must obtain approval and licensing from the CMA. To be eligible for licensing, the crowdfunding platform operator should be a company limited by shares with a minimum paid-up capital of $10,000. The licence will be issued to the eligible operator once they meet all the requirements including an application fee of $100 as well as an annual regulation fee of $200.

f. A platform operator will be deemed to operate in Kenya if:
   i. the crowdfunding platform is established in Kenya;
   ii. the platform is located outside Kenya but actively targets Kenyan investors; or
   iii. the key components of the platform are physically in Kenya even if any of its components are located outside Kenya.
g. The CMA may suspend, restrict or revoke a crowdfunding platform operator licence in accordance with the Capital Markets Act. In addition, a person operating a crowdfunding platform in Kenya without a licence commits an offence under these regulations and is liable to a penalty amounting to $100,000 for corporations and $50,000 for natural persons. The platform operator will be responsible for ensuring that the funds raised through the platform are used for the stated objective. The crowdfunding platform operator is also mandated to appoint a financial institution duly registered by the CMA as a custodian, who shall establish and maintain a separate trust account for each funding round on its platform.
h. Crowdfunding transactions – a crowdfunding offering shall not remain open for more than 60 days and where an issuer is unable to meet the prescribed minimum threshold for the targeted amount, the offer shall be withdrawn and the crowdfunding platform operator shall effect a refund of the monies to the investors within 48 hours. The issuer may only commence a fresh crowdfunding offering no earlier than 90 days after the said withdrawal. However, where the crowdfunding transaction is successful, the crowdfunding platform operator shall make the funds available to the issuer within 24 hours after the close of the offer.

Moreover, investors are granted a "cooling-off" period of 48 hours, which is the period within which the investor can withdraw an offer or agreement to purchase the securities or investment instrument by delivering a notice to the crowdfunding platform operator. A platform operator is expected to prepare and display a warning statement on the crowdfunding platform to all visitors using the platform, to investors, and on all application investment forms. Investors must then sign the risk acknowledgment form to confirm that they understand that the risks of the proposed investment, that they will never be able to sell the security, that they will be provided with minimal disclosure and that they will not have the benefits of protection associated with the investment.

Indeed, the regulations are a commendable move by the National Treasury and the CMA as they will ensure that investors using crowdfunding platforms are protected and that the raising of finances on crowdfunding platforms is controlled. These regulations will also enhance accountability and transparency of operations on the crowdfunding platforms and will ensure the supervision of crowdfunding operations by the CMA. The regulations are also aimed at ensuring that investors' funds are used for the stated purpose by holding the platform operator responsible for ensuring that the funds raised through the platform are used for the outlined objective. The other key advantage is that this provides another avenue for businesses to seek funding and diversify their funding sources from traditional financial institutions such as banks.

Regulatory Sandbox

The CMA's Regulatory Sandbox, launched in March 2019, presented its Milestone Report and this is discussed further below.

Intergovernmental Fintech Working Group

In a bid to position for future outcomes, the CMA Soundness Report 2021 highlighted the steps taken in South Africa with regard to bringing crypto assets into the purview of

regulation. It is clear from this report that Kenya is positioning itself to regulate crypto assets and that South Africa is a good benchmarking jurisdiction.

In South Africa, the Intergovernmental Fintech Working Group, through the Crypto Assets Regulatory Working Group, published a position paper on crypto assets, focusing its attention on certain key areas, including that crypto assets will be brought into the South African regulatory purview in a phased and structured manner across three main areas:

1. Anti-money laundering and combatting the financing of terrorism (AML/CFT).
2. Cross-border financial flows: From an exchange control perspective, the current Exchange Control Regulations do not explicitly cater for crypto assets, with the implication that the South Africa Reserve Bank's Financial Surveillance Department does not have explicit powers to require South African crypto asset trading platforms to report transactions involving crypto assets.
3. Application of financial sector laws: Given the increased retail interest in crypto assets, growing instances of consumer abuse, fraud and market misconduct have been noted both internationally and in South Africa. Recent schemes highlighted in the media further emphasised the need for South African authorities, predominantly through the Financial Sector Conduct Authority, to act against the growing tendency for market abuse under the guise of crypto assets.

From the elaborate leanings of the South African government, the CMA has concluded that multi-stakeholderism with other financial regulators in Kenya is imperative, the most important being the CBK. In particular, we must look into how specific crypto assets may now be brought under each organisation's regulatory ambit.[10]

The year was not devoid of scammers, however, and the CMA flexed its muscles and put out a cautionary warning against investing in a particular online Bitcoin trading company in Kenya. According to the regulator, the company was luring the public into investing in products while promising a return of 400% within six hours. The CMA requested that any investor who has been defrauded to report to the nearest law enforcement authorities with the relevant documents, including any contract that was entered into to support the claim.[11] Therefore, without a solid legal framework that governs digital assets in Kenya with clear sanctions, the CMA is relegated to issue cautionary statements and rely on existing criminal law for recourse as investor protection mechanisms.

The CBK

Following its Annual Supervision Report 2020, the CBK stated with regard to cryptocurrency and blockchain (digital ledger technologies) that there is a budding interest in cryptocurrencies driven by their potential use as a medium of exchange.

The CBK stressed that cryptocurrencies had garnered significant attention over the last seven to nine years, resulting in growing debates and concerns over the efficacy and economic use of cryptocurrencies. The report acknowledged that research to demystify cryptocurrencies had been conducted by organisations such as the Financial Stability Board, the Bank for International Settlements, the Committee on Payments and Market Infrastructures, the Basel Committee on Banking Supervision, the European Union and the G20.

The research emphasised that there is no clear evidence that cryptocurrencies present material risks to financial stability and monetary policy at this stage. However, continuous monitoring of the size and growth of cryptocurrencies is prudent to ensure that their material risks are identified as well as their transmission channels to financial stability risk. In conclusion, the CBK is inclined to work in tandem with other financial sector regulators, and will continue to inform the public of the potential risks posed by cryptocurrencies.[12]

However, contrary to its conclusions discussed above, the CBK is yet to regulate the space or provide guidance on the same. The Bank prohibited the use of traditional financial institutions to transact with crypto-based companies, never provided an alternative, and no action is being undertaken. This was further evident through its draft Kenya National Payments System Vision and Strategy, 2021–2025, which invited comments from the public, and in which there was no mention of crypto/virtual currencies.[13]

In summation, cryptocurrencies are still not regulated in Kenya nor are they backed by the government or the CBK, and therefore they are not recognised.

Cryptocurrency regulation

In Kenya, there are still no specific cryptocurrency laws and so the general regime of the law applies.[14] In addition to the regulation discussed in the previous edition of this book, the following law was enacted in 2021 and will form the core consideration of how to deal with data on the blockchain.

The Data Protection Act

The Kenya Data Protection Act, 2019 (DPA) has been in force for over a year, and the first Data Commissioner (DC) was appointed in November 2020. After the appointment, the DC commenced the formalities of setting up the office and now that things have settled down, enforcement of the provisions of the DPA has commenced.

Due to the varied interpretation of the provisions of the DPA, it was necessary for the privacy regulator to issue follow-up regulations and guidelines. These are aimed at the implementation aspect of the provisions of the DPA. The regulations also contain the official forms to be used as required by the DPA. Last year, the DC's office issued the following guidelines:

1. Data Protection Impact Assessment guidelines.
2. Guidance Note on Consent.
3. Complaints Management Manual.[15]

In April 2021, the office issued the following further draft guidelines, which are now subject to public participation before adoption:

1. Data Protection (Compliance & Enforcement) Regulations, 2021.
2. Data Protection (Registration of Data Controllers & Data Processors) Regulations, 2021.
3. Data Protection (General) Regulations, 2021.[16]

These draft regulations are timely since, in the last year, data controllers and processors have adopted different ways of implementing the DPA in their business procedures to achieve some sort of compliance. This is because the DPA became enforceable immediately upon its enactment, unlike the EU General Data Protection Regulation (GDPR), which became enforceable two years after its adoption.[17]

The DPA mirrors the GDPR and it would be interesting to see how it will be applied locally in Kenya by data controllers/processors for organisations using blockchain technology. It is appreciated that blockchains are a class of technology. Indeed, there is not simply one version of this technology. Rather, the term refers to many different forms of distributed database that present much variation in their technical and governance arrangements and complexity. Compatibility between distributed ledgers and the DPA can only be assessed on the basis of a detailed, case-by-case analysis that accounts for the specific technical design and governance set-up of the relevant blockchain use case.

Two critical elements to be appreciated about data in a blockchain *vis-à-vis* the DPA are the following:

1. First and foremost, the foundation of the DPA, just like the GDPR, is based on the assumption that in relation to each personal data point there is at least one natural or legal person – the data controller – whom data subjects can address to enforce their rights. Contrary to this assumption, blockchains often seek to achieve decentralisation by replacing a singular actor with many different players. This then begs the question of how we apportion the responsibility and accountability burden, particularly in light of the uncertain delineations of the concept of (joint) controllership under the DPA.
2. Secondly, it is assumed that data can be modified or erased where necessary to comply with legal requirements, such as Section 40 of the DPA. Blockchains, however, render such modifications of data burdensome in order to ensure data integrity and to increase trust in the network. Again, the uncertainties pertaining to this area of data protection law are increased by the existing uncertainty in the DPA. For instance, what happens to the "erasure" principle?

It is clear that these tensions play out in many domains. For example, does data typically stored on a distributed ledger, such as public keys and transactional data, qualify as personal data for the purposes of the DPA? Specifically, the question is whether personal data that has been encrypted or hashed still qualifies as personal data. It is often assumed that this is not the case; however, such data likely does qualify as personal data for DPA purposes, meaning that the DPA will apply where such data is processed.

More broadly, this analysis also highlights the difficulty in determining whether data that was once personal data can be sufficiently "anonymised" to meet the DPA threshold of anonymisation captured under Part IV "Obligations of Data Controllers and Data Processors", in particular Regulation 18 "Retention of personal data". Another example of the tension between blockchain and the DPA relates to the overarching principles of data minimisation and purpose limitation under Regulation 35 "Categories of notifiable data breach". Whereas the DPA requires that personal data that is processed be kept to a minimum and only processed for purposes that have been specified in advance, these principles can be hard to apply to blockchain technologies. Distributed ledgers are append-only databases that continuously grow as new data is added. In addition, such data is replicated on many different computers. Both aspects are problematic from the perspective of the data minimisation principle.

Furthermore, it is unclear how the "purpose" of personal data processing ought to be applied in the blockchain context, specifically whether this only includes the initial transaction or whether it also encompasses the continued processing of personal data (such as storage and its usage for consensus) once it has been put on-chain. It is the tension between the right to erasure (the "right to be forgotten") and blockchains that has probably been discussed most in recent years. Indeed, blockchains are usually deliberately designed to render the (unilateral) modification of data difficult or impossible. This, of course, is hard to reconcile with the DPA's requirements that personal data must be amended (under Regulation 9 "Right to rectification") and erased (under Regulation 11) in specific circumstances, all captured in Part IV "the Right of a Data Subject".

In conclusion, there are very technical specificities and governance designs of blockchain use cases that can be hard to reconcile with the DPA. Therefore, blockchain architecture for any specific organisation from the outset needs to be designed in a manner that ensures compliance with the DPA.

Sales regulation

Pursuant to the Warning Notice issued by the CBK in 2015, it neither prohibits the sale of cryptocurrencies nor does it legitimise it. Hence, it is clear that the sale of virtual currencies and tokens in Kenya is not prohibited or regulated. It is noteworthy that in relation to the craze of non-fungible tokens (NFTs), the famous Kenyan marathoner, Eliud Kipchoge, sold his first set of NFTs for a total of ETH 17,9837 on the largest NFT marketplace, OpenSea. Kipchoge is considered the greatest marathoner of all time for being the first human in history to run a sub-two-hour marathon as part of the INEOS 1:59 Challenge in 2019 in Vienna.[18]

Taxation

Despite the inclination to tax cryptocurrencies through the Finance Act, 2019 amendment to the Income Tax Act of Kenya, it remains to be seen what the impact will be on individual users targeted by the new taxes as well as firms, both large and small. In all likelihood, large companies such as Zoom – which has started paying VAT on its services in Kenya – will weather the storm. However, service taxes, for example, could be a heavy weight for struggling start-ups that shifted into the digital space for survival. This could have the effect of stifling the young, local digital industry.

Money transmission laws and anti-money laundering requirements

The Eastern and Southern Africa Anti-Money Laundering Group (ESAAMLG) is among the eight Financial Action Task Force (FATF)-style regional bodies that form part of the FATF's global network.

One of the biggest threats perceived by regulators is that some cryptocurrency transactions are completely anonymous. While there is a huge opportunity presented by cryptocurrencies to transfer "money" cheaply and quickly, there is a significant risk for nefarious characters to take advantage of the system, notably for money laundering and terrorism financing objectives. The question then is how will regulators oversee this in a manner that promotes the financially inclusive capabilities of cryptocurrency, while also preserving national security interests?

Kenya subscribes to international standards of AML/CFT. It is a member of the FATF under the auspices of the ESAAMLG, whereas locally the statutory underpinning is the Proceeds of Crime and Anti Money Laundering Act (POCAMLA). This Act provides for mandates to entities with regard to reporting and monitoring obligations. This is supported by various Circulars issued by the CBK in this regard, notably Circular No. 1 of 2018 and Circular No. 2 of 2019 relating to AML/CFT, respectively. The Circulars detail the requirements of the CBK to financial institutions to provide comprehensive evidence of their compliance with regulations relating to AML/CFT. The aim of this and other recent CBK instructions is to strengthen the integrity of the country's financial systems. Section 45(2) of POCAMLA requires reporting institutions to execute customer due diligence (CDD) on existing customers or clients at all times and with vigilance. While POCAMLA does not define CDD expressly, in practical terms, banks acquire access to international resources and instruments, which are specifically developed specially by the FATF for CDD. POCAMLA grants reporting institutions the ability to exercise stricter check-ups and reports. In Kenya, all reporting institutions are subject to POCAMLA and must show that the person they are dealing with actually exists. Also, they must be able to identify those persons who are mandated to undertake the transactions, on their behalf or on behalf of others. Banks and other reporting institutions have to conduct the CDD in such a way that they will be able to

explicitly identify the business operations and transactions with the customer in the future. Enhanced customer due diligence (ECDD) is not internationally defined. Nonetheless, it is clear that ECDD is a process of investigation, which is rigorous and robust over and above know-your-customer (KYC) procedures. Its goals are the verification and validation of the customer's actual identity, as well as comprehending and testing the customer's data.

This begs the question whether the same requirements apply for cryptocurrencies and whether virtual asset providers operating in Kenya should be included as reporting institutions. The drafting of POCAMLA is very broad and may include entities that employ blockchain technology, but sadly it is not explicit.

The Act provides that the Cabinet Secretary in charge of Finance may "designate such other business or profession in which the risk of money laundering exists..., to have to comply with the reporting and monitoring obligations"; to wit: cryptocurrencies.

Furthermore, POCAMLA is not restricted to money as it also includes "property", which has a broad definition and, to an extent, Fintech innovations would fall under said definition. The operators of some Fintech innovations that include the transfer of money or value may be deemed to be "reporting institutions" under the POCAMLA and have reporting and compliance obligations.

Blockchain technology poses a challenge with regard to compliance with KYC provisions. Practical recommendations would include: outsourcing the data validation function to external entities that can certify or validate the data being put into the blockchain, while responsibility and corresponding liability for compliance remains with the regulated entity; and using blockchain explorer software.

However, POCAMLA is silent on whether KYC due diligence obligations can be outsourced to third parties. That said, it does specifically prohibit the outsourcing of KYC due diligence obligations when transacting with jurisdictions that have been designated as high risk or are otherwise monitored by the FATF.[19]

Promotion and testing

In 2019, the CMA set up a Regulatory Sandbox to help it gain insight into new innovations and facilitate live testing, in essence to reduce the risk to consumers from new financial products and services. Selection into the Sandbox is guided by international practices and the CMA's Regulatory Sandbox Policy Guidance Note.

In April this year, the CMA released a report on its Regulatory Sandbox. In its introduction, the report was to take note of the achievements realised and to reflect on the lessons learnt since it began operating in March 2019. To provide some background, the idea of the Sandbox was conceptualised in 2014, with the launch of the 10-year Capital Market Master Plan (CMMP). At the time, one of the main outcomes that the CMMP sought was to stimulate innovation that would broaden the products and services offered in the capital markets, deepen market participation and liquidity, and drive transformative economic development.[20]

Key features of the report highlighted the following challenges experienced by the Sandbox Team:

1. Technical incapacity of the Team resulted in it having to go out of its way to try to understand the products and solutions before they could be approved for admission into the Sandbox. To mitigate this, the Team engaged in constant consultation and capacity building, working with applicants and other partners to overcome this challenge.

2. Divergent views or positions taken by fellow regulators in the financial and other sectors have made the process of reviewing certain applications quite taxing, especially where the applications contain aspects that are cross-cutting. This is especially a problem because regulators are at different levels of embracing Fintech solutions or ideas. There have been concerted efforts towards convergence in approach especially for financial sector regulators.
3. The Joint Financial Sector Regulators Forum constituted a working group on collaboration in promoting adoption of technology and innovation in the financial services sector to enhance effective regulation and supervision. This is expected to play a key role in enhancing convergence in thinking and developing a common front in the approach towards the regulation of Fintech. The financial system is highly interconnected, diversified and segmented with increased cross-border operations. The adoption of Fintech has transformed the sector in terms of products and services through innovations. The complexity of the financial sector has resulted in the establishment of non-operating holding companies to manage operations of these complex entities. While this transformation and growth in complexity has brought efficiency and synergies in resource use and profit maximisation, it has also become a growing source of potential risk, including fraud and cybersecurity attacks. However, the financial system was generally stable in 2019, and has been able to withstand the macro financial shock resulting from the COVID-19 pandemic.
4. Some Fintech solutions are under review given their newness and novelty, and due to the fact that there are not many jurisdictions to benchmark against and compare notes with. This was further compounded by fear of the likely consequences of disruption in the market, such as disintermediation. There has not been a comparable market or jurisdiction to benchmark against.
5. In the realm of decentralised finance, blockchain solutions, cryptocurrency and its derivatives, the pressing challenges were exhibited as follows:
    a. Novelty and complexity of the concept.
    b. Insufficient information regarding the risk universe in this area.
    c. Lack of internal capacity to review these types of applications.
    d. Objections of Central Banks to issue cryptocurrencies.
    e. Fears around volatility affecting local currency.
    f. Concerns around cybersecurity and data safety.
    g. The challenge of multiple Fintech firms providing a solution to solve the same common problem.
6. Tokenisation brought its own set of challenges, including:
    a. Delinking tokenisation from cryptocurrency.
    b. Grappling with the idea of stablecoins and other regulators' opinions on the same lack of clarity on custodial arrangements of the assets.
    c. Verification and valuation of the assets.
    d. How to handle market bifurcation where there may exist two markets for the same asset (on-chain and off-chain).
    e. Concerns around cybersecurity and data safety.

There is still a lot to be explored with the Sandbox and we hope this will be reflected in the next Milestone Report.

Ownership and licensing requirements

Owing to the ruling in *Wiseman Talent Ventures Ltd*, cryptocurrencies are treated as securities, and this is regarded as the current position.

Mining

Mining is not prohibited; however, despite an implication that such activities would attract digital services tax at 1.5%, said tax has not yet been implemented. Earnings from mining activities are naturally subject to existing laws and regulations that attract income tax payments, and are undertaken within the current regulation as long as they do not promote or encourage prohibited activities.

Border restrictions and declaration

Fortunately, or unfortunately, there are no definite obligations to declare cryptocurrency holdings. Nevertheless, any declarations would naturally be included as part of the existing regime of laws where such declarations would be expected.

Reporting requirements

No report has been updated on this. It is clear that Kenya does not have specific cryptocurrency payment declarations. In addition to the POCAMLA and the CBK guidelines and regulations on AML/CFT, the Kenya Association of Bankers issued guidelines on transactions above $10,000, notably that any amounts beyond that shall require approval from the respective bank and, if higher, from the regional heads of the banks. These safeguards over fiat currency are likely to apply to cryptocurrencies as well, but the same are tweaked within the crypto space as per each individual exchange; for example, under Paxful, a cryptocurrency exchange and a player within the Kenyan space has various KYC requirements depending on the amount of money being traded.

Estate planning and testamentary succession

The legal status of cryptocurrencies and the extent to which you can "own" an intangible digital asset is still uncharted ground within the Kenyan legal space. The anchoring legislation is Chapter 160 of the Law of Succession Act, which stipulates how a deceased person's estate will be distributed.

Despite the lack of a legal framework for digital inheritance, which would, among other things, address the definition, scope and transfer of digital assets, and facilitate intestate succession, the Kenyan Judiciary is appreciative of the new World Order we find ourselves in. Digital estate is defined to include digital media and rights that can be inherited. This is an important and emerging area of inheritance practice worldwide and Kenya is no exception.

Digital assets are (in contrast to physical assets) more dynamic and ephemeral. When a person dies, they leave behind a digital presence, which can include online accounts, passwords, contracts, receipts, financial transactions, medical information and personal websites, and can involve banking, writing, images and social media. A digital estate is not only a person's online presence, but also includes data stored digitally on personal technology such as a phone or computer. Digital assets are ephemeral and subject to constant change. The definition is wide enough to cover cryptocurrencies.

Kenya, like the rest of the world, has witnessed the growth of digital assets, and digital inheritance is therefore an important issue as its population has largely gone digital with mobile penetration being at over 90%, mobile subscriptions up to 39.7 million, and smart phone uptake at 40%.

The number of registered mobile money accounts increased from 61.7 million at the end of June 2020 to 67.8 million at the end of June 2021, an increase of over 6 million. Similarly,

the volume of mobile money transactions increased from 143.1 million in June 2020 to 175.8 million in June 2021, a factor that has contributed to Kenya being ranked highly in digital financial inclusion.[21]

Kenya's mobile money transactions jumped to $30.3 billion between January and June 2021, a 52% increase from $19.2 billion in the same period in 2020, according to data from the CBK. Based on the CBK data, Kenyans transferred on average $165.3 million each day through their mobile phones in H1 2021, thanks to the increased uptake of e-Commerce services and a shift from cash to mobile-based payments.

Kenya is poised to becoming a fully fledged digital economy. This spread provides for large volumes of digital media and related digital assets, and accordingly questions of inheritance of those assets.

Currently, there is no universal definition of a digital asset or digital estate. However, they are basically such digital media that one owns or has rights to, and are mainly information stored in an intangible medium on computers or other computer-related technology. The prevalence of an individual's online presence can increase the number of assets available for transfer to heirs, thereby affecting access to valuable property.

In Kenya, however, there is no law addressing the inheritance of digital assets/property. This legislative gap affects the following areas: defining the assets and their scope; managing these assets; ascertaining; accessing; privacy; transfer; and disposing. Some ideas that are being considered in digital asset mapping for estate planning in developed jurisdictions such as the US include: personal and business emails; attachments to emails; business websites; records of the sort that were formerly kept in a safe deposit box and are now stored online or digitally; digital pictures stored on your camera, on CDs or online; online brokerage or bank accounts; as well as libraries of music, movies, games, and software.

One major challenge to inheritance of digital assets is access. Service agreements made between service providers and users are important in determining who may get access to a digital asset. An internet business can, however, change its service agreement with or without notice, creating added complications for an heir attempting to access or even delete a family member's account.

A personal representative or beneficiary may even be unable to delete the deceased's account as a way of managing/disposing of it, just as the deceased may have been unable to delete it due to a service agreement. Digital assets such as social networking sites can also be difficult to access. For example, Gmail has a policy through which anyone may be able to access a deceased person's mail if he or she can provide proof that the "user is known to be deceased". Further, Yahoo's terms of service "explicitly states that an account cannot be transferred". This may mean that the property in the account asset is not transferable, and therefore cannot be considered to be the user's property transmissible at death.[22]

This raises the question as to the current scope of property rights in digital assets. For instance, do unlimited property rights to digital accounts, such as email accounts, exist only during a person's lifetime and terminate upon his or her death? Potential loss of digital assets is also a major concern. For example, "individuals spend enormous amounts of money over their lifetimes purchasing files for their iTunes account, so a deceased's iTunes account could potentially represent a substantial asset". However, iTunes files are non-transferable upon a user's death and therefore cannot be transferred.[23] Lack of direct access to this type of digital asset could lead to a loss in a person's estate, since this type of asset will not be included in any estate planning as actual property. And cryptocurrencies are no exception; it is imperative that a legal framework be put in place in order to protect

these digital assets. In the interim, one is encouraged to keep a list of digital accounts and wealth with trusted family members knowing where they are. However, this should be kept securely and separate from passwords to avoid causing security issues if the information ever gets into the wrong hands. It should therefore not be included in the Will, as the Will becomes a public document if and when probate is granted. It also needs to be easy to access so it can be updated given this ever-changing area.

* * *

Endnotes

1. https://bitcoinke.io/2021/06/localbitcoins-in-africa-report-compilation/.
2. https://bitcoinke.io/2021/08/zero-deposit-fees-localbitcoins/.
3. https://blog.chainalysis.com/reports/2021-global-crypto-adoption-index.
4. https://bitcoinke.io/wp-content/uploads/2020/05/The-State-of-Crypto-in-Africa-The-May-2020-Luno-Report.pdf.
5. https://www.capitalfm.co.ke/business/2021/02/akoin-launches-in-kenya-with-promise-for-alternative-continent-wide-currency/.
6. https://www.grassrootseconomics.org/sarafu-network; https://kenyanwallstreet.com/the-kenya-red-cross-launches-sarafu/.
7. https://www.cma.or.ke/index.php?option=com_phocadownload&view=category&id=38&Itemid=196.
8. http://kenyalaw.org/caselaw/cases/view/182238.
9. Capital Market Soundness Report – Q2 2021: https://www.cma.or.ke/index.php?option=com_phocadownload&view=category&id=5&Itemid=261.
10. https://www.cma.or.ke/index.php?option=com_content&view=article&id=727:cautionary-statement-against-fxbitinvest&catid=12:press-center&Itemid=207.
11. https://www.centralbank.go.ke/uploads/banking_sector_annual_reports/1375903848_Bank%20Supervision%20Annual%20Report%202020.pdf.
12. https://twitter.com/CBKKenya/status/1343449348374487041; https://www.centralbank.go.ke/2020/12/23/invitation-for-public-comments-on-the-draft-kenya-national-payments-system-vision-and-strategy-2021-2025/.
13. https://www.globallegalinsights.com/firms/njogu-and-associates/muthoni-njogu.
14. Data Protection Act, 2019: https://www.Kenyalaw.org.
15. https://www.odpc.go.ke/download/odpc-complaints/.
16. https://www.odpc.go.ke/.
17. https://gdpr-info.eu/.
18. https://runningmagazine.ca/the-scene/eliud-kipchoge-career-highlights-sold-as-nfts-for-50000/.
19. Proceeds of Crime and Anti Money Laundering Act, 2012.
20. https://www.cma.or.ke/index.php?option=com_content&view=article&id=708:cma-launches-regulatory-sandbox-milestones-report-2&catid=12&Itemid=207.
21. https://bitcoinke.io/2021/07/mobile-money-transactions-in-kenya-yoy/.
22. https://www.google.com and https://www.yahoo.com deceased users account.
23. https://appleinsider.com/articles/21/01/02/what-to-do-about-apple-devices-and-icloud-content-when-the-ownerdies.

Muthoni Njogu
Tel: +254 725 615 596 / Email: mnjogu@njoguassociates.com

Muthoni Njogu is the Managing Partner and Head of Commercial & Corporate Law. Her practice areas include Corporate & Commercial, Civil & Commercial Litigation, Dispute Resolution, Technology, Media & Telecommunications, and Intellectual Property. She has a wealth of experience in both the public and private sectors where she has served for the last 11 years, including offering legal advice to local and multinational entities in banking, information technology and manufacturing industries. She is a certified Mediator for the Mediation Training Institute, a Chartered Arbitrator from the Chartered Institute of Arbitrators (CIArb), a Commissioner for Oaths, and a Notary Public. In addition, she is also deeply passionate about the 4IR, notably blockchain and virtual currencies, and is a speaker on matters of blockchain and digital asset regulation.

Njogu & Associates Advocates

House No. 246A, Owashika Road, Off Isaac Gathanju Road, Lavington, 40493-00100 Nairobi, Kenya
Tel: +254 725 615 596 / URL: www.njoguassociates.com

Korea

Won H. Cho & Dong Hwan Kim
D'LIGHT Law Group

Government attitude and definition

General overview

The major updates to the Virtual Asset-related regulations in Korea are as follows:

(a) The enforcement of the Amended Act on the Reporting and Using Specified Financial Transaction Information Act ("SFIA"), which contains information regarding Virtual Asset Service Providers ("VASPs").
(b) The passing of a taxation bill regarding the taxation of individual Virtual Asset transactions (to be enforced from January 1, 2022).

In Korea, the SFIA, which contains information on Virtual Assets (as defined below) and VASPs, was enforced on March 25, 2021. The enforcement of VASPs' reporting obligations under the SFIA has been deferred to September 24, 2021, and other regulations regarding VASPs are continuously being arranged to this day. The major amendments to the SFIA are as follows:

(a) Definition of "Virtual Asset" and "Virtual Asset Service Provider".
(b) Imposition of reporting obligations on VASPs.
(c) Imposition of anti-money laundering ("AML") obligations on VASPs.

In order to report a VASP, an Information Security Management System ("ISMS") certificate, which is a security-related certification, must be obtained. Moreover, if a VASP intends to provide exchange services that exchange fiat currency (such as KRW) and Virtual Assets, the VASP must establish a verifiable real-name account at a domestic bank; however, domestic banks are taking a very cautious stance in issuing such verifiable real-name account services to VASPs. The SFIA also applies to overseas corporations whose business is targeted at Korean citizens; accordingly, it is extremely challenging for an overseas business operator who constitutes a VASP under the SFIA to provide exchange services that exchange fiat currency and Virtual Assets to Korean citizens.

The establishment of Virtual Asset-related laws and regulations in Korea has somewhat been delayed compared to other countries. The SFIA is a law that imposes AML/CFT-related (anti-money laundering and combatting the financing of terrorism) obligations on financial companies. The recent amendment to the SFIA set forth regulations on VASPs by imposing reporting obligations on them.

The National Assembly is actively discussing promotion acts that are currently pending in relation to Virtual Asset businesses; however, at this time, there are no laws prescribed for VASPs other than the SFIA.

The Korean government has consistently held a cautious stance towards Virtual Asset businesses in Korea since 2017 and is actively implementing a policy that promotes blockchain technology by separating Virtual Assets from blockchain technology.

The work related to Virtual Assets and blockchains is divided amongst the following government ministries:

Department	Related Matters
Financial Services Commission ("FSC")	Management, supervision and improvement of systems regarding VASPs, such as AML, etc., to enhance transparency of transactions
Ministry of Economy and Finance	Operation of support teams, taxation of Virtual Assets, inspection of violation of the Foreign Exchange Transactions Act, etc.
Ministry of Science and ICT	Fostering of blockchain industry, prevention of VASP hacking, etc.
Prosecutors and other investigative agencies	Crime control, such as frauds using Virtual Assets, etc.
Fair Trade Commission	*Ex officio* investigation of unfair terms and conditions of VASPs
Personal Information Protection Committee	Responding to leakage and infringement of personal information of participants to a Virtual Asset transaction
National Tax Service	Preparation for implementation of the Virtual Asset taxation system, coercive collection of Virtual Assets of high-value delinquents, etc.
Korea Customs Service	Supervision of violation of the Foreign Exchange Transactions Act, such as use of Virtual Assets in foreign exchanges, etc.

Cryptocurrency regulation

Definition under the SFIA

Before March 25, 2021, when the amended SFIA of March 24, 2020 was enforced, Korea lacked a clear legal definition of cryptocurrency or Virtual Assets. Various governmental authorities and regulatory bodies have issued guidelines and publications proposing the standards by which Virtual Assets should be regulated; nevertheless, the SFIA was the first legislation that defined Virtual Assets into law in Korea.

Under the SFIA, a Virtual Asset is "an electronic token with economic value that is tradable or transferrable electronically (including any rights to the Virtual Asset) that excludes:

(1) token or information about a token that cannot be exchanged by monies, commodities, or goods and services and the use and place of which has been restricted by the issuer;
(2) tangible and intangible items acquired through game products as provided under Article 32(1)(7) of the Gaming Industry Promotion Act;
(3) electronic prepayment means under Article 2(14) and electronic currency under Article 2(5) of the Electronic Financial Transactions Act;
(4) electronically registered stock, etc., under Article 2(4) of the Act on the Electronic Registration of Stocks, Bonds, Etc.;
(5) electronic bills under Article 2(2) of the Issuance and Distribution of Electronic Bills Act;
(6) electronic bills of ladings under Article 862 of the Commercial Act;
(7) electronic bond under Article 2(16) of the Electronic Financial Transactions Act;
(8) gift certificates stored and used on mobile devices such as mobile phones in which the issuer sets the amount of money or the quantity of the goods or services that can be used; and
(9) other items that conform with Article 1 and Article 2 of the SFIA that the commissioner of the Korea Financial Intelligence Unit announces to be excluded as a Virtual Asset in consideration of the type and characteristics of the transaction" (none have yet been announced).

The SFIA does not impose any restrictions on the purpose of use of Virtual Assets. Accordingly, the definition of Virtual Assets provided by the SFIA is much broader than the

definition provided by the Financial Action Task Force. Moreover, the SFIA defines Virtual Assets by explicitly prescribing the exception to what constitutes a Virtual Asset. Under the SFIA, a so-called "security token" may be considered a Virtual Asset even if it constitutes a security since it is not explicitly excluded from the definition of Virtual Asset. Accordingly, security tokens may simultaneously be subject to the SFIA and the Financial Investment Services and Capital Markets Act ("Capital Markets Act"), which governs laws on securities.

The SFIA defines VASPs as follows and requires VASPs to report to the commissioner of the Korea Financial Intelligence Unit ("KoFIU"). The issuance of Virtual Assets has been excluded from the operation of VASPs, which seems to reflect the financial authorities' position in effectively prohibiting initial coin offerings ("ICOs"). The Korean government's position on ICOs is stated in the "Sales regulation" section below.

A VASP is defined as a person who engages in the business of any one of the following:
(1) selling and purchasing of Virtual Assets;
(2) exchanging of Virtual Assets for another Virtual Asset;
(3) transferring of Virtual Assets to transact, exchange, store, or maintain, etc., the Virtual Assets following a request from a customer;
(4) storing or managing of Virtual Assets; or
(5) brokering, intermediating, or acting as an agent with regard to any transactions under clause (1) or (2).

A VASP who fails to comply with the obligation to report as a VASP or who reports by false information or other illegal means may be sentenced to up to five years in prison and/or fined up to KRW 50 million.

VASP reporting requirements

As stated above, the SFIA is the only domestic legislation that regulates Virtual Assets at the time of writing. However, the SFIA does not directly regulate Virtual Assets except for a few dark coins. The SFIA regulates Virtual Assets by regulating VASPs who operate businesses that use Virtual Assets.

The financial authorities may reject a VASP's report if their requirements are not met. Accordingly, VASPs should be vigilant in meeting the following requirements when reporting to the KoFIU. The following describes VASP reports that may be rejected:
(1) those who fail to obtain an ISMS certificate;
(2) those who do not transact through a verifiable real-name account (an account that only allows financial transactions between an account of a VASP with an account of another VASP in the same finance company, etc. (this is limited to finance companies prescribed in the Presidential Decree)). However, this does not apply to cases where there is no exchange in Virtual Assets and fiat currencies regarding the Virtual Asset transaction by a VASP for its customers;
(3) those who have been sentenced to more than a fine under a finance-related law, and five years have not passed since the end of the execution or the exemption of the sentence; and
(4) those who have reported or have changed a report using false statements or other fraudulent methods and have had their reports or changes cancelled in accordance with the SFIA, and five years have not passed since the cancellation.

All VASPs must obtain ISMS certifications, which are supervised by the Korea Internet & Security Agency ("KISA"), a public institution under the Ministry of Science and ICT. Moreover, there are no legal standards for the issuance of verifiable real-name accounts. Banks have the sole discretion of evaluating an individual VASP's risks and issuing a

verifiable real-name account. VASPs that do not provide services that exchange Virtual Assets with fiat currencies do not need verifiable real-name accounts.

Furthermore, through their press releases, the financial authorities are classifying certain VASPs as "Major VASPs". On February 17, 2021, the FSC issued a Manual on VASP Reporting, which defined "Major VASPs" as (i) Virtual Asset Trading Service Providers, (ii) Virtual Asset Safekeeping and Administrative Service Providers, and (iii) Virtual Asset Digital Wallet Service Providers. They further provided that, in the case of Major VASPs, the SFIA would apply clearly, and depending on the type of business operation, other businesses may also be considered VASPs. The different types, meanings, and reasons for the exclusion of Major VASP candidates suggested by the government are as follows:

- *Virtual Asset Trading Service Providers*: A Service Provider who operates a platform to a broker or intermediates the sales and exchanges, etc., of Virtual Assets (Virtual Asset trading businesses, exchange businesses, and exchanges).
- *Virtual Asset Safekeeping and Administrative Service Providers*: A Service Provider who operates a business of storing and managing the Virtual Assets on behalf of others (Virtual Asset custodies, consignment businesses).
- *Virtual Asset Digital Wallet Service Providers*: A Service Provider who provides storage, management, and transfer services for Virtual Assets (centralised wallet services, trust-type wallet services, wallet services).

Common reasons for exclusion:

- Services that simply provide a platform to post proposals of sales and purchases of Virtual Assets (in the event that they simply operate a bulletin board that states that Virtual Assets are available for use, but uses a separate wallet, not related to a person or an entity related to the bulletin board to transact between the parties).
- Services that simply provide advice or technology regarding Virtual Asset transactions.
- Services in which the Service Provider does not engage in the transfer, storage, or exchange of Virtual Assets as it does not have independent control over personal encryption keys and only provides a program to store the Virtual Assets.
- Cold wallet providers or hardware wallet service manufacturers, etc.

Regulations on foreign VASPs

The SFIA has regulations that have extraterritorial effect, which allows the application of the law to extend beyond Korea if an act performed overseas has an effect in Korea. Accordingly, even a VASP located in a foreign country must report to the KoFIU if it engages in a business targeting Koreans in Korea; and, with regard to the operation of its business with Koreans, it must be performed in accordance with the obligations set forth in the SFIA. Here, the criteria used to determine whether one is engaged in a business directed at Koreans is determined by comprehensively considering whether (i) the business provides the services in Korean language, (ii) there is marketing or publicity targeted at Koreans, or (iii) the business supports payments and transactions in KRW.

On July 22, 2021, the financial authorities reclarified such obligations of foreign VASPs and delivered letters to foreign VASPs, including Binance, whom they believed were operating businesses targeting Korean audiences, emphasising their reporting obligations under the SFIA.

Pre-announcement of the amendment to the Enforcement Decree of the SFIA

The Enforcement Decree of the SFIA (subordinate laws) will be amended, and the contents of the main amendments are as follows:

(1) Prohibition of handling Virtual Assets issued by oneself or by a person with a special relationship under the Commercial Act.

(2) Prohibition of VASPs and their employees from transacting Virtual Assets through the respective VASP.

This amendment seeks to prevent price manipulation of Virtual Assets through market making, etc., in Virtual Asset exchanges and to prevent the general public from suffering harm while transacting Virtual Assets.

Sales regulation

Overview

In the event a person sells Virtual Assets that do not constitute a security such as Bitcoin or Ethereum in Korea, he must report himself as a VASP as a "person who engages in the business of selling Virtual Assets". However, the financial authorities have prohibited ICOs in effect; therefore, one must be careful when selling tokens through a Korean entity. Moreover, depending on the nature and method of the sale of Virtual Assets, one must be careful about violating the Capital Markets Act, the Act on the Regulation of Conducting Fund-Raising Business Without Permission, and the Act on Door-to-Door Sales, Etc.

Financial authorities' attitude towards ICOs

Historically, the financial authorities have banned ICOs for several reasons, such as to protect investors, and to this day, ICOs are still prohibited in effect. "Prohibited in effect" means that the ICO is not prohibited or restricted by law *per se*; however, if the financial authorities find an ICO case in Korea, they will strictly investigate whether any violations surround the said ICO.

The government has taken a cautious stance regarding the systemisation of ICOs for investor protection reasons; accordingly, teams that develop decentralised applications or issue tokens in Korea have conducted their businesses by establishing their corporations abroad. The Korean government stated that investors face high risks of damages due to the lack of transparent information regarding ICOs, and many other major issues, including: (i) the lack of information about the developer; (ii) the difficulty of the project content and the non-transparent nature of the process; (iii) the undisclosed details of the use of ICO funds; and (iv) the non-transparency of the developer's profile.

Moreover, the government warned that a licence may be required under the Capital Markets Act when the platforms are used to issue or trade peer-to-peer loan securitisation tokens, sell funds that invest in Virtual Assets, or issue security tokens. Moreover, any exaggerated advertisements regarding the value of a token or any major matter at an ICO or to a potential platform participant may constitute fraud under the Criminal Act.

Regulations under the Act on the Regulation of Conducting Fund-Raising Business Without Permission

The Act on the Regulation of Conducting Fund-Raising Business Without Permission defines "fund-raising business without permission" as any business that is performed to raise funds from unspecified individuals by promising to pay them an equal or greater amount of the principal amount without obtaining authorisation or permission or making a registration or report, etc., under other Acts and subordinate statutes.

Accordingly, any sale of Virtual Assets and Virtual Asset-related products with a promise of an equal or greater amount of value of the said Asset in the future without a separate licence regarding the financing will be in violation of the Act on the Regulation of Conducting Fund-Raising Business Without Permission.

In relation to this, any services or products provided on the premise of staking may be penalised for being a violation of the Act on the Regulation of Conducting Fund-Raising

Business Without Permission, as it is structured to pay interest in addition to the deposited Virtual Assets. Any agreement to pay more than the principal amount would be considered a financing act subject to the Act. For example, paying tokens and allowing them to be exchanged for fiat currency in the future, or paying a bonus in accordance with the result of sales, or promising a profit at the expiration of a specific period, will be considered fund-raising acts rather than the sale of goods or products and punished as "fund-raising business[es] without permission".

Taxation

Accounting of Virtual Assets

At the time of writing, the Korea International Financial Reporting Standards ("K-IFRS") and the general corporate financial reporting standards do not specify any regulations or guidelines on Virtual Assets. However, South Korea has been adhering to the announcement made by the International Accounting Standards Board and the K-IFRS Interpretations Committee in June 2019 and applying the respective provisions *mutatis mutandis*. Under these provisions, Virtual Assets are accounted as (i) inventories if they are held for sale or traded for brokerage in the course of normal business operations, and (ii) intangible assets in all other cases. According to the disclosed financial statuses of large Virtual Asset exchanges in Korea that have a duty to disclose their financial situation, Virtual Assets are indeed being accounted as inventories, and each Virtual Asset is calculated and accounted for under a fair internal standard.

Taxation on Virtual Asset transactions

From January 1, 2022, taxes will be imposed on profit gains from the sales of Virtual Assets. The Income Tax Act classifies income generated from Virtual Asset transactions as other income, and more specifically, as "other income subject to separate taxation", which is not included when calculating the tax base of global income. In other words, the profit gains from the sales of Virtual Assets are not included when calculating an individual's global income tax.

The regulations on applicable tax rates differ depending on whether one is a resident (under the Income Tax Act, any individual who has their domicile or place of residence in the Republic of Korea for at least 183 days) or a non-resident (any individual who is not a resident) of South Korea. For residents, the tax rate (final tax amount) for Virtual Assets is calculated separately based solely on their Virtual Asset income by subtracting KRW 2.5 million from their Virtual Asset income, and thereafter multiplying the amount by 0.2 (in other words, 20%; additionally, a 10% local tax is imposed on the final tax amount, totalling 22% of the Virtual Asset income). Since this is not subject to tax withholding, the parties to a Virtual Asset transaction must report their Virtual Asset income by themselves in May each year.

Non-residents are only subject to taxation if their transactions are recognised as domestic transactions, such as transactions through domestic exchanges. As with residents, the income derived from domestic Virtual Asset transactions of non-residents are classified as "domestic source other income", and in the event that a non-resident transfers, leases, or withdraws Virtual Assets through a VASP, the VASP withholds the lesser of (a) 20% of the gains from the Virtual Asset transfer, or (b) 10% of the payment amount as tax. Since non-residents are taxed in the form of withholding tax, the withholding agent who remits the Virtual Asset income to the non-resident withholds the tax amount when remitting the Virtual Asset income to the non-resident and is required to pay the withheld tax to the tax offices by the 10th of the month following the month the tax was withheld. Here, the "Virtual Asset income to be withheld when withdrawing Virtual Assets" means the market

price of the Virtual Asset minus necessary expenses and the acquisition value. Accordingly, if there are no confirmed necessary expenses or acquisition value, 10% of the payment amount will be calculated as the Virtual Asset income amount.

Since taxation on profit gains from sales of Virtual Assets will be enforced from 00:00 am on January 1, 2022, any withdrawal of Virtual Assets after 00:00 am on January 1, 2022 will be subject to the said tax regime. Accordingly, the "deemed acquisition value" will be used to determine the price of each Virtual Asset as of 00:00 am on January 1, 2022, and the Virtual Assets will be deemed to have been acquired at such Virtual Asset price as of that time. The "deemed acquisition value" will be the greater of (a) the average value of the Virtual Asset price announced by the VASPs who were announced by the commissioner of the National Tax Service (the announcement on the list of VASPs for this year has not yet been announced), or (b) the actual value at which the holder acquired the Virtual Asset.

Money transmission laws and anti-money laundering requirements

A VASP's duty to verify its customers

In order to engage in the business of Virtual Asset transactions, one must report oneself as a VASP under the SFIA. For more information, please refer to the "Cryptocurrency regulation" section above.

If a customer transfers Virtual Assets worth KRW 1 million or more to another VASP in a single transaction, the VASP must provide the following information at the time of the transaction:

(1) The name of the sender and his/her Virtual Asset address.
(2) The name of the recipient and his/her Virtual Asset address.

In addition, the VASP must collect the sender's resident registration number, passport number, or foreign registration number, and, if requested by the KoFIU or the VASP of the corresponding recipient, provide the information within three business days from receipt of the request. VASPs are obligated to store the collected customer information for five years from the date the financial transaction is completed.

Other AML obligations of VASPs

VASPs have AML obligations. More specifically, VASPs must take the following measures:

(1) Separately manage transaction details for each customer.
(2) Separately manage customer deposits and the VASP's proprietary property.
(3) Limit transactions for customers whose verification procedures have not been completed.
(4) Must not transact with VASPs who have not met their reporting obligations for any business purposes.
(5) Must not broker the sale or exchange of Virtual Assets between a customer and a customer of another VASP. However, a VASP may broker such transaction if the other VASP has fulfilled its AML obligations and has undergone the proper licence, permit, registration, and reporting procedures in Korea or abroad, and the following are implemented:
    (a) if the other VASP is licensed abroad, a copy of the certificate of the licence issued by the foreign government must be submitted to the commissioner of the KoFIU; and
    (b) the VASP must verify and record information on the customer of the other VASP who is transacting with the VASP's customer daily and submit a report on the verification procedure and method to the commissioner of the KoFIU in advance.
(6) Verify whether the Virtual Asset is a Virtual Asset whose transfer record cannot be identified because of internal technologies that prevent the transfer record from being identified when a Virtual Asset is transferred from one Virtual Asset address to another; and if not, make sure that the Virtual Asset is not processed.

In the case of item (5), it is intended to limit order book sharing and linking between the Virtual Asset exchanges, which was initially banned without exception. Nevertheless, due to strong opposition from the industry, order book sharing has now been made possible under certain conditions with VASPs licensed abroad.

Promotion and testing

The Korean government is actively supporting and fostering research and development ("R&D") activities in blockchain technology through various R&D investments and government-led blockchain projects. KISA, a public institution under the Ministry of Science and ICT, and the National IT Industry Promotion Agency ("NIPA") are conducting blockchain pilot projects in various fields, and the Institute of Information & Communications Technology Planning & Evaluation is conducting various projects on the development of blockchain technology.

The sandbox system is active in Korea, and there are various examples of sandbox designations that use blockchain technology. Busan Metropolitan City is designated as a Special Regulatory Free Zone for the blockchain sector in the regulatory sandbox system that eases regulations on a particular industry in a specific region, designated pursuant to the regulatory sandbox system. There are a total of seven projects designated under this regulatory sandbox ("Special Cases"), including a digital ledger-based local currency activation service, a blockchain-based real estate collective investment and revenue allocation service, and a blockchain-based non-face-to-face healthcare and mydata platform.

Since April 2019, a total of 21 Special Cases in the financial regulatory sandbox operated by the FSC have also applied blockchain technology.

However, unlike its positive stance on blockchain technology, the Korean government continues to take a negative stance on the sale of Virtual Assets. Accordingly, there are no specially designated businesses or cases for Virtual Assets in a more conventional sense.

In addition, the Bank of Korea stated that it would proceed with its central bank digital currency simulation research project in August 2021, which will continue until June 2022 over two stages.

Ownership and licensing requirements

Virtual Assets are not specified in the Capital Markets Act, which prescribes investment and asset management regulations. However, the Capital Markets Act defines "collective investment" as the "investing [of] money, etc. pooled from at least two investors, or any surplus funds to acquire, dispose of, and manage by any other method investable assets with property value in a manner that does not receive ordinary management instructions from the investors or fund management entities, and distributing the yields therefrom to vest in the investors of fund management entities". Virtual Assets constitute "money, etc." and "any other asset with property value". Accordingly, any collective investment using Virtual Assets will constitute a collective investment business under the Capital Markets Act and require authorisation from the FSC.

Mining

Currently, there are no regulations on Virtual Asset mining. However, the Capital Markets Act may apply to a mining business if it engages in financing activities for its business in Korea. Furthermore, if the business sells Virtual Assets obtained through mining for fiat

currency, etc., the business will be considered "a business that engages in the sale of Virtual Assets" and reporting obligations as a VASP will be imposed. For more information on VASPs, please refer to the "Cryptocurrency regulation" section above.

Border restrictions and declaration

There are no clear regulations on Virtual Assets under the Foreign Exchange Transactions Act, and foreign exchange banks are not accepting any reports regarding the remittance of Virtual Assets.

Nevertheless, arbitrage transactions have been actively taking place in Korea due to the difference in the Virtual Asset price between overseas Virtual Asset exchanges and domestic Virtual Asset exchanges, and the term "Kimchi Premium" has been coined to describe this phenomenon. Accordingly, a number of overseas remittances have been made to obtain the profit gains from the sale of Virtual Assets from these arbitrage transactions, and if KRW is to be remitted overseas for the purposes of a Virtual Asset transaction, the existing Foreign Exchange Transactions Act will apply as is, through which the Foreign Exchange Transactions Act may be violated, and penalties may be imposed.

For example, under the Foreign Exchange Transactions Act, any person who intends to perform a capital transaction must file a report on such capital transaction with the Minister of Economy and Finance. Small transactions that are exempt from such reporting obligations are: (i) transactions where the payment amount is within USD 5,000 (in the case of payment in instalments, the sum of all instalments is within USD 5,000); or (ii) capital transactions in excess of USD 5,000 and less than or equal to USD 50,000 per transaction, with an annual cumulative total less than or equal to USD 50,000, etc. In any case, if the unreported amount of a capital transaction exceeds KRW 1 billion, one may be sentenced to up to one year in prison and/or fined up to three times the value of the violation amount. If the unreported amount is less than KRW 1 billion, a fine of up to KRW 100 million may be imposed.

Therefore, any overseas remittance or receipt of assets for the purposes of Virtual Asset transactions without filing a report to the Minister of Economy and Finance may constitute a violation of the Foreign Exchange Transactions Act even if it does not fall under any of these exceptions. For example, if several hundred small remittances are made to a non-resident, whether the transactions violate the Foreign Exchange Transactions Act will depend on whether the transactions are made in the form of instalments of a capital transaction.

Reporting requirements

VASPs have an obligation to keep records of customers whose Virtual Asset transactions are over the amount of KRW 1 million, and if the customer is a VASP, the VASP has an obligation to provide such information to the VASP customer. There are no other obligations that require the VASPs to report to the Bank of Korea or the KoFIU when the Virtual Asset transaction amount is over a certain amount. However, similar to other financial institutions, VASPs must report any suspicious transactions to the KoFIU as soon as they come to their knowledge. For more information, please refer to the section above on "Money transmission laws and anti-money laundering requirements".

Estate planning and testamentary succession

There are no established laws or court precedents regarding Virtual Assets under current inheritance laws in Korea. Under the Civil Act, the inheritance of Virtual Assets occurs

automatically, but the successor faces difficulties in processing the inherited Virtual Assets since third parties (including the government or other individuals), other than the individuals who have access to the keys to the Virtual Asset wallet, do not have access to the Virtual Assets.

The absence of a way to access the Virtual Asset wallet through coercive means signifies that the government cannot exercise its authority to forcefully dispose of the Virtual Assets, which causes several issues, such as difficulties in seizing assets and collecting forfeitures.

However, if Virtual Assets are deposited in a Virtual Asset exchange, which usually holds the right to access the said Virtual Assets, seizures, confiscations, and forfeitures of the deposited Virtual Asset may take place. Accordingly, it is likely that Virtual Assets that are deposited in VASPs who can access the customer's Virtual Assets, such as Virtual Asset exchanges or custody Service Providers, are likely to be inherited.

Won H. Cho
Tel: +82 2 2051 1870 / Email: whc@dlightlaw.com

As an experienced patent lawyer with extensive commercial transactional experience in various specialty industries including entertainment, ICT and healthcare, Won H. Cho is uniquely positioned to advise clients on a wide range of complex IP, corporate and regulatory matters. He started his career as an associate at Bae, Kim & Lee LLC ("BKL") and went on to serve as a partner of the firm, leading BKL's prominent IP and technology transaction practices, spanning a total of 16 years. Mr. Cho also worked on secondment at Ropes & Gray (New York) in 2014 in the firm's IP division. Recently, he has been actively advising clients in the blockchain industry.

Mr. Cho is now an adjunct professor at KAIST-MIP (Master of Intellectual Property) and serves in leadership roles at various local and state organisations, including the Korea Fair Trade Commission Advisory Committee, the Korean Intellectual Property Office, the US-Korea Law Foundation, the Licensing Executive Society Korea, and the Korea Entertainment Law Society, among others. Mr. Cho holds a B.A. from Seoul National University and received an LL.M. from the University of Texas at Austin.

Dong Hwan Kim
Tel: +82 2 2051 1870 / Email: dhk@dlightlaw.com

Dong Hwan Kim, a Korean attorney at D'LIGHT, has advised a wide range of companies leading the Fourth Industrial Revolution encompassing blockchain, big data/AI, fintech and so forth. In particular, Mr. Kim has professional expertise in smart contracts and various protocols, based upon which he has hitherto rendered advisory services on whether blockchain technology-based companies would be deemed virtual asset service providers and consulting services about business models, while representing such clients before financial authorities for their notification requirements. Furthermore, Mr. Kim has served as a project manager for consulting and legal advisory matters of the NIPA for its ICT regulatory sandboxing projects since 2020. With such experience, he is considered a renowned specialist with a profound understanding of how the Korean regulatory reform policies and sandbox systems work.

D'LIGHT Law Group

5th Floor, 311, Gangnam-daero, Seocho-gu, Seoul, 06628, Republic of Korea
Tel: +82 2 2051 1870 / Fax: +82 2 2051 1877 / URL: www.dlightlaw.com

Luxembourg

José Pascual, Bernard Elslander & Clément Petit
Eversheds Sutherland LLP

Government attitude and definition

The Luxembourg financial centre has a forward-looking approach, establishing itself as Europe's number one international fund distribution platform with international outreach. The Government of the Grand Duchy of Luxembourg keeps this approach in the FinTech industry, aiming at being Europe's pioneer in the blockchain world[1] alongside developing a dedicated national FinTech platform:[2] the Luxembourg House of Financial Technology (the "**LHoFT**").[3] Charged with building and fostering Luxembourg's burgeoning FinTech ecosystem, the LHoFT brings together financial institutions, FinTech innovators, research, academia and public authorities, to help drive forward the development of products that meet specific industry needs.

Further, the regulatory authority that oversees Luxembourg's financial sector, the *Commission de Surveillance du Secteur Financier* (the "**CSSF**"), acknowledges the financial benefits of blockchain technology, and Luxembourg's Minister of Finance, Mr. Pierre Gramegna, has spoken of the "*added value and efficient services*"[4] that cryptocurrencies bring.

This innovative approach is further undertaken in the context of the publication of the digital finance package adopted by the European Commission on 24 September 2020 (the "**Digital Finance Package**") including the proposals for a regulation on the markets in cryptographic assets ("**MiCA**"), on digital operational resilience for the financial sector ("**DORA**") and on a pilot regime for market infrastructure based on distributed ledger technology (the "**Pilot Regime**"). The Digital Finance Package was welcomed in Luxembourg by the *ad hoc* working group on digital finance strategy of the Association of the Luxembourg Fund Industry ("**ALFI**") in its position paper,[5] while also advising certain clarifications or amendments to be carried out in the draft proposals.

With regard to the definition of virtual asset, the CSSF has published no interpretative guidance. Thus, in absence of specific regulations, any person engaging in activities related thereto or implied through the creation of tokens or the collection and raising of funds shall, depending on their characteristics, assess whether they are subject to certain legal provisions in Luxembourg and thus to certain supervisory requirements. This assessment is strongly recommended and shall be facilitated by the medium of the Innovation Hub, a newly established division within the CSSF as described in the *Promotion and testing* section below.

According to the European Securities and Markets Authority's ("**ESMA**") Advice on Initial Coin Offerings and Crypto-Assets (the "**ESMA Advice**"), a crypto-asset is "*a type of private asset that depends primarily on cryptography and Distributed Ledger Technology* ("**DLT**") *or similar technology as part of their perceived or inherent value. Unless otherwise stated,*

ESMA uses the term to refer to both so-called 'virtual currencies' and 'digital tokens'. Crypto-asset additionally means an asset that is not issued by a central bank".[6]

Although ESMA does not define the term "*virtual currency*", this term has been introduced in Article 1(20a) of the Luxembourg law of 12 November 2004 on anti-money laundering and counter-terrorist financing (the "**AML/CFT Law**") following the implementation of Directive 2018/843 of 30 May 2018 on the prevention of the use of the financial system for the purposes of money laundering: "*[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 persons as a means of exchange and which can be transferred, stored and traded digitally.*"[7]

The ESMA Advice provides that a digital token is "*any digital representation of an interest, which may be of value, a right to receive a benefit or perform specified functions or may not have a specified purpose of use*".

According to the CSSF, "*digital tokens (…) may, where applicable, grant certain rights to their holders. These rights are freely defined by the initiator and may take different forms, such as the provision of a service, a share in the capital of the company being formed, the right to a part of the profit or the right to receive a manufactured product*".[8] This definition corresponds to the traditional classification of crypto-assets given by the European Banking Authority ("**EBA**"):[9] utility tokens; security tokens; investment-type tokens; and payment tokens.

Cryptocurrency regulation

Even though there is no legal framework in Luxembourg that specifically applies to virtual currencies, the CSSF issued a warning on virtual currencies on 14 March 2018[10] indicating that any provision of financial services requires authorisation by the Minister of Finance.

In another warning issued on the same date relating to initial coin offerings ("**ICOs**") and tokens,[11] the CSSF acknowledged that raising funds from the public in the form of ICOs is not subject to specific regulation and does not benefit from any guarantee or other form of regulatory protection. The CSSF considered that despite the lack of specific regulations applying to ICOs, activities related to the creation of tokens and the collection and raising of funds may, depending on their characteristics, be subject to certain legal provisions and thus to a number of supervisory requirements.

The CSSF specified in this second warning that it would "*assess such fundraising activities by extending its analysis to the objectives pursued in order to assess whether it could be a scheme to circumvent or avoid financial sector regulations, notably the provisions of the Law of 10 July 2005 on prospectuses for securities and the Law of 5 April 1993 on the financial sector. The CSSF considers that for any fundraising, the initiators of such ICOs are required to establish anti-money laundering and terrorist financing procedures*".[12] For more details on the applicable framework in relation to anti-money laundering and counter-terrorist financing, please refer to the *Money transmission laws and anti-money laundering requirements* section below.

The CSSF warning on virtual currencies was in line with ESMA's position on ICOs,[13] which considered that as the coins or tokens used as crypto-assets may qualify as financial instruments, firms involved in ICOs must carefully consider whether their activities, such as placing, dealing in or advising on financial instruments or managing or marketing collective

investment schemes, constitute regulated activities. Moreover, they may be involved in offering transferable securities to the public.

This position was later confirmed in the ESMA Advice dated 9 January 2019.[14]

From a Luxembourg perspective, this means that activities related to crypto-assets may fall within the scope of the law of 5 April 1993 on the financial sector, as amended (the "**Financial Sector Law**"), the Luxembourg law of 30 May 2018 on markets in financial instruments, the Luxembourg law of 17 December 2010 relating to undertakings for collective investment, the Luxembourg law of 12 July 2013 on alternative investment fund managers (the "**AIFM Law**"), the Luxembourg law of 10 November 2009 on payment services, and the Luxembourg law of 16 July 2019 on prospectuses for securities (the "**Prospectus Law**").

Tokens could be based on or represent a unit in an alternative investment fund and thus trigger the compliance of this instrument with the AIFM Law. With respect to UCITS and other regulated funds targeting non-professional customers and pension funds, the CSSF indicated that the latter will not be permitted to invest directly or indirectly in tokens through ICOs.

Where a token qualifies as a financial instrument within the meaning of the Financial Sector Law, the provision of investment and ancillary services in and from Luxembourg may trigger the requirement to obtain prior written authorisation from the CSSF, including, *inter alia*, to act as portfolio manager, investment adviser, underwriter of financial instruments, or broker in financial instruments.

If a token qualifies as a security within the meaning of Article 4(1)(44) of Directive 2014/65/EU on markets in financial instruments ("**MiFID II**") and is offered to the public or admitted to trading on a regulated market, the issuance of such token will not be permitted without the publication of a prospectus that has been approved by the CSSF under the Prospectus Law.

Finally, where a token matches the definition of electronic money within the meaning of the law of 10 November 2009 on payment services, as amended (the "**Payment Services Law**"), the issuer must apply for a licence or registration with the CSSF to provide services or issue electronic money.

Sales regulation

Issuers offering tokenised securities or security tokens to the public will have to draft a prospectus in compliance with Regulation 2017/1129/EU on the prospectus to be published when securities are offered to the public or admitted to trading on a regulated market (the "**Prospectus Regulation**") and the Prospectus Law.

In this context, it is worth mentioning that the Prospectus Regulation exempts security offers to the public with a total consideration in the European Union of less than EUR 1 million, calculated over 12 months from the obligation to publish a prospectus.[15]

An additional exemption may apply, as the Prospectus Regulation offers Member States the option not to require the publication of a prospectus for offer or securities to the public not exceeding EUR 8 million over a 12-month period, but only to the extent such offering is limited to one single Member State and such offerings shall not benefit from the passporting regime.

Other exemptions provided in the Prospectus Regulation relate, for example, to:

a. offers made to qualified investors, or offers addressed to fewer than 150 persons per Member State (other than qualified investors);

b. offers of securities whose denomination per unit amounts to at least EUR 100,000; or
c. offers addressed to investors who acquire securities for a total consideration of at least EUR 100,000 per investor for each separate offer.

Sales of unregulated tokens (these are tokens that do not qualify as financial instruments under MiFID II) should be exempt from the obligation to publish a prospectus.

In addition to sale regulation that arises out of the Luxembourg financial regulatory framework, there is a draft of general advertising, online/distance selling and consumer protection legislation that is potentially applicable to sale of crypto-assets or the offering of services related to crypto-assets (such as exchange or wallet) in or from Luxembourg.

Some, like the Consumer Code (*Code de la consommation*), only apply in relation to consumers (typically defined as individuals acting outside of their trades, business, craft or profession) but where they do, provide consumers with significant statutory rights and remedies against supplies of goods, services and digital content and impose restrictions on the kinds of contractual terms that can be enforced against consumers. Others, like the law of 14 August 2000 on electronic commerce, are of more general application and impose requirements on business establishments in Luxembourg that offer or provide goods and services digitally. The application of such legislation may also depend on whether or not the business being conducted is subject to Luxembourg financial regulation.

Taxation

In recent years, the Luxembourg tax authorities aimed at clarifying the direct taxation and VAT treatment of cryptocurrencies.

Luxembourg income taxation

In a circular published on 26 July 2018 regarding virtual currencies, the Luxembourg tax authorities highlighted that a cryptocurrency is not a currency, it is not legal tender and its value is not monitored by any central bank.[16] Therefore, for direct tax purposes, it constitutes an intangible asset, meaning that companies will not be allowed to draw up their financial statements or to file their tax returns in cryptocurrencies.

This circular goes on to state that when a cryptocurrency is used as a payment method, the nature of the income will not be affected. This means that, for example, where rent is paid in virtual currency, it does not affect the nature of rental income.

When income is derived from disposing of the cryptocurrency itself, taxation of such income does not depend on whether it has been accrued in the real or virtual world, but whether the derived income is commercial income or "other income".

The income derived from cryptocurrencies will constitute "commercial income" providing that it meets the conditions set out in Article 14 of the Luxembourg law dated 4 December 1967 on income tax: "*Any independent activity, with a profit-making intention, exercised on a permanent basis, which participates in the general economy, when said activity is neither a forestry activity nor an independent professional activity*." In this respect, there are three categories of taxpayers:

Category 1: Luxembourg corporate taxpayers

Luxembourg corporate taxpayers carry on a commercial activity. Therefore, the gains of such taxpayers derived from the disposal of cryptocurrencies will constitute commercial income. Such commercial income will be fully taxable at a combined corporate income tax and municipal business tax rate of 24.94% (combined tax rate for a corporate taxpayer based in Luxembourg City).

Category 2: Luxembourg individual taxpayers

The gain realised on the disposal of cryptocurrencies by Luxembourg individual taxpayers carrying on a commercial activity will constitute commercial income. Such income will be taxable at the progressive tax rates applicable for personal income tax, varying from 0% to 42%.

If the Luxembourg individual taxpayer does not carry on a commercial activity, the gain realised on the disposal of cryptocurrencies should be considered "other income". If this "other income" is realised within six months after the acquisition of the cryptocurrency, such income will be considered a speculative gain and will be fully taxable at the applicable progressive tax rates for personal income, varying from 0% to 42%. However, if the gain is realised six months after the acquisition of the cryptocurrency, such gain will be exempt from Luxembourg personal income tax.

Category 3: Luxembourg partnerships

Luxembourg partnerships are tax transparent from a Luxembourg tax perspective unless they are considered to carry on a commercial activity. Under this context, a Luxembourg partnership not carrying on a (deemed) commercial activity should not be subject to Luxembourg taxation for the gains realised on disposal of cryptocurrencies. However, if a Luxembourg partnership is considered to realise commercial income, such commercial income will be subject to municipal business tax at a rate of 6.75% (for a Luxembourg partnership based in Luxembourg City).

Value-added tax

In addition, in June 2018, the Luxembourg VAT authorities published Circular No. 787 regarding exemption for virtual currency transactions, stating that the VAT exemption applicable to transactions concerning currency used as legal tender would extend to virtual currencies, to the extent that they are regarded as a method of payment and are accepted for this purpose by some operators.[17]

Money transmission laws and anti-money laundering requirements

The Luxembourg legislator recently implemented two new laws on 25 February 2020 and on 25 March 2021 to strengthen the anti-money laundering and counter-terrorist financing framework. These laws amend the AML/CFT Law and introduce new registration and governance requirements for virtual asset service providers ("**VASPs**"), which must be maintained in a register (the "**Register**") established by the CSSF and published on its website.

For the purpose of the AML/CFT Law, VASPs, "virtual asset" and custodian wallet service providers are defined as follows:

- **VASPs**: all entities providing one or more of the following services on behalf of their clients or for their own account:
  a. exchange between virtual assets and fiat currencies, including the exchange between virtual currencies and fiat currencies;
  b. exchange between one or more forms of virtual assets;
  c. transfer of virtual assets;
  d. safekeeping and/or administration of virtual assets or instruments enabling control over virtual assets, including custodian wallet services; and
  e. participation in and provision of financial services related to an issuer's offer and/or sale of virtual assets.
- **Virtual asset**: a digital representation of value, including a virtual currency, that can be digitally traded or transferred, and can be used for payment or investment purposes,

except for virtual assets that fulfil the conditions of electronic money within the meaning of point (29) of Article 1 of the Payment Services Law and the virtual assets that fulfil the conditions of financial instruments within the meaning of point (19) of Article 1 of the Financial Sector Law.[18]

- **Custodian wallet service providers**: a service consisting of safekeeping private cryptographic keys on behalf of clients for the purpose of holding, safekeeping and transferring virtual currencies.[19]

For the purpose of registration with the Register, VASPs must send a request to the CSSF, together with the following information:

a. the name of the requesting entity;
b. the address of the central administration of the requesting entity;
c. a description of the services provided and the activities performed, and the list of the specific virtual asset services provided; and
d. a description of the money laundering and terrorist financing risks that the requesting entity will be exposed to and of the internal control mechanisms that the requesting entity implements to mitigate those risks, and to comply with the professional obligations included in the AML/CFT Law and in Regulation (EU) 2015/847 on information accompanying transfers of funds.[20]

To successfully obtain registration, a VASP must submit evidence of the professional repute of the individuals exercising management functions in the VASP and its ultimate beneficial owners ("**UBOs**") to the CSSF. There must be at least two individuals exercising management functions who must be empowered to effectively determine the direction taken by the business and possess adequate professional experience. Any change to the UBOs or individuals exercising management functions must be pre-approved by the CSSF.

The CSSF has the right to remove the entity from the Register in case of non-compliance with certain obligations and has the power to impose administrative sanctions and other administrative measures in the AML/CFT Law.

In December 2020, the Ministry of Justice[21] published an AML/CFT risk assessment and identified as high risks some characteristics of certain types of virtual assets, such as the possibility of pseudonymous or anonymous transactions.

This has been tackled by the implementation of the law of 25 February 2021, which amended the AML/CFT Law. The amendment has clarified the list of information and documentation required for the official registration of VASPs in Luxembourg and has added the explicit obligation of demonstration of professional honourability and adequate professional expertise for all natural persons responsible for the management of the VASP. Further evolution will be awaited in this regard with the implementation in Luxembourg of the AML/CFT package published by the European Commission on 20 July 2021, including a new AML/CFT regulation and a recast of Regulation (EU) 2015/847 of the European Parliament and of the Council of 20 May 2015 on information accompanying transfer of funds, which would extend the information requirements currently applying to wire transfers to crypto-assets, and force VASPs to collect and make accessible data concerning the sender and the beneficiary of transfers of virtual assets.

Promotion and testing

In line with its technology-neutral position, the CSSF chose not to regulate the underlying technology or the cryptocurrencies themselves, but rather the service providers who offer financial services involving cryptocurrencies.

The first European exchange platform, Bitstamp, which enabled customers to exchange Bitcoin against EUR and USD and *vice versa*, was authorised by the Luxembourg Minister of Finance in April 2016 to operate EU-wide bases under a payment institution licence. One of the largest exchanges in the world – bitFlyer – received its Luxembourg licence in December 2017, becoming the first Bitcoin exchange to be licensed on three continents.

Additionally, the first real estate tokenisation was completed with blockchain technology in Luxembourg in 2019 with the support of Luxembourg-based service providers, which demonstrates the eagerness of the CSSF to welcome similar transactions.[22]

Importantly, the CSSF published a brochure on 8 February 2021, "*Financial Innovation: a challenge and an ambition for the CSSF*",[23] announcing the creation of a new division within its innovation, payments, market infrastructure and governance department (the "**Innovation Hub**"). In order to encourage an open dialogue with the Innovation Hub, the CSSF further published a form to be used for presenting an innovative project with the possibility to obtain feedback on regulatory requirements.[24]

This new CSSF division specialises in crypto-assets, payments and e-money, artificial intelligence, robo-advice and crowdfunding. The establishment of the Innovation Hub is of utmost importance for actors in the crypto-assets market in Luxembourg, as it constitutes a specific point of contact for any query in relation to DLT, virtual/crypto-assets and virtual/crypto-asset service providers.

From a technical perspective, standardisation is also key in implementing and using any technology. As part of the Luxembourg Standardization Strategy 2020–2030, the *Institut Luxembourgeois de la Normalisation, de l'Accréditation, de la Sécurité et Qualité des Produits et Services* (the "**ILNAS**") released a new national technical standardisation report, "Blockchain and distributed ledgers".[25] The ILNAS, as a public administration under the authority of the Minister of Economy, provides an overview of the distributed ledger normative landscape and highlights the initiatives available at the European and international level for national actors to get involved in technical standardisation.

Ownership and licensing requirements

From the perspective of evidencing ownership, this section focuses on how Luxembourg's legal framework for the issuance and circulation of securities encourages the use of new technologies in financial services.

In this context, we analyse the three different forms of securities existing under Luxembourg laws and develop an analysis of the most suitable forms for tokenisation among the following:

a. bearer securities (*titres au porteur*), which are the less common form of securities and are thus not discussed hereafter;
b. registered securities (*titres nominatifs*), the most common form of securities in Luxembourg companies being subject to the provisions of the Luxembourg law of 10 August 1915 on commercial companies, as amended (the "**1915 Law**") and the Luxembourg Civil Code; and
c. dematerialised securities (*titres dématérialisés*) as defined in the Luxembourg law of 6 April 2013 on dematerialised securities (the "**2013 Law**").

Registered securities are created through an inscription in a register of security holders in application of the provisions of the 1915 Law and even though nothing in the 1915 Law prevents the use of a DLT as a register for the issuance, transfer and recording of registered securities, the absence of DLT-specific provisions under Luxembourg law advocates for the use of dematerialised securities.

Dematerialised securities have been introduced by the 2013 Law, which defines which securities can be dematerialised (subject to certain exceptions):[26]

- capital securities issued by joint-stock companies under Luxembourg law, including shares and stock, beneficiary shares, subscription rights and common fund units; and
- debt securities subject to Luxembourg law such as financial instruments likely to be in the form of bearer instruments and public debt instruments.

The 2013 Law further enables Luxembourg companies and investment funds to issue securities in dematerialised form and convert existing registered or bearer securities into dematerialised securities.

Additionally, the implementation of the Luxembourg law of 1 March 2019 increased legal certainty by expressly permitting securities to be maintained by the account keeper through secured electronic registration mechanisms, including DLT such as blockchain (the "**2019 Law**").

A key principle arising out of the commentary to the 2019 Law[27] is technological neutrality. Under this principle, the 2019 Law recognised the possibility of using different types of "*secured electronic registration mechanisms*", not just distributed electronic registers or databases (i.e. blockchain), allowing flexibility in relation to new technologies.

More recently and as part of the ongoing modernisation of Luxembourg's legal framework, the Luxembourg law of 22 January 2021 (the "**2021 Law**") amended the Financial Sector Law as well as the 2013 Law. In particular, the 2021 Law (a) confirms the possibility to issue dematerialised securities directly in DLT devices, and (b) broadens the access to the activity of the central account keeper (*teneur de comptes central*) with respect to unlisted debt securities to EEA credit institutions and investment firms, provided they meet certain specific organisational and technical requirements.

As to licensing requirements, and as mentioned in the *Money transmission laws and anti-money laundering requirements* section above, all virtual assets and custodian wallet service providers, or "VASPs" as defined in the AML/CFT Law, must be added to the dedicated Register.

Mining

There are no restrictions in Luxembourg on the mining of cryptocurrency, provided that the production of such virtual currencies/crypto-assets does not fall within the scope of any specific statutory licensing obligation. Please refer to the "*Sales regulation*" section above.

Border restrictions and declaration

In line with the CSSF warning regarding virtual currencies, which states that "*given the cross-border character of VC transactions, establishing a national regulation would only have limited effects*", there are no specific border restrictions or any obligations to declare cryptocurrency holdings under Luxembourg law.

Reporting requirements

Under Luxembourg law, there is currently no reporting requirement for crypto-asset payments regardless of transaction value. Nevertheless, VASPs must comply with the provisions of the AML/CFT Law, which provides that, *inter alia*, when a VASP has reasonable grounds to suspect or suspects that a transaction can be linked or related to AML/CFT activities, it is obliged to report suspicious activity and suspicious transactions to the Luxembourg financial intelligence unit (*Cellule de Renseignement Financier*).

Estate planning and testamentary succession

Under Luxembourg law, there is no special treatment for crypto-assets for the purposes of estate planning and testamentary succession, and crypto-assets should be treated like any other assets in such situations.

* * *

Endnotes

1. 'Luxembourg Aims To Be Europe's Pioneer In The Blockchain World' (*Government of the Grand Duchy of Luxembourg*, 7 July 2021) https://luxembourg.public.lu/en/invest/innovation/blockchain.html.
2. 'Fintech – Shaping the future of finance' (*Luxembourg for Finance*, 30 January 2019) https://www.luxembourgforfinance.com/en/financial-centre/fin-tech/.
3. Luxembourg House of Financial Technology: https://lhoft.com/en/.
4. Pierre Sorlut, '*Ce qu'en pense le ministre des Finances – Les monnaies virtuelles, un phénomène incontournable*' (*Luxemburger Wort*, Luxembourg, 31 August 2018).
5. 'Position paper on MiCA, DORA, and the Pilot Regime' (*ALFI*, 18 June 2021) https://www.alfi.lu/Alfi/media/Statements/2021/ALFI_Position_Paper_on_MiCA_DORA_and_the_Pilot_Regime_20210622.pdf.
6. 'Advice on Initial Coin Offerings and Crypto-Assets' (*ESMA*, 9 January 2019) Appendix I: https://www.esma.europa.eu/sites/default/files/library/esma50-157-1391_crypto_advice.pdf.
7. Law of 12 November 2004 on the fight against money laundering and terrorist financing transposing Directive 2001/97/EC of the European Parliament and of the Council of 4 December 2001 amending Council Directive 91/308/EEC on prevention of the use of the financial system for the purpose of money laundering.
8. 'Warning regarding Initial Coin Offerings and Tokens' (*Commission de Surveillance du Secteur Financier*, 14 March 2018) https://www.cssf.lu/en/2018/03/warning-regarding-initial-coin-offerings-icos-and-tokens/.
9. 'Report with advice for the European Commission on crypto-assets' (*EBA*, 9 January 2019) p.7: https://www.eba.europa.eu/sites/default/documents/files/documents/10180/2545547/67493daa-85a8-4429-aa91-e9a5ed880684/EBA%20Report%20on%20crypto%20assets.pdf?retry=1.
10. 'Warning regarding virtual currencies' (*Commission de Surveillance du Secteur Financier*, 14 March 2018) https://www.cssf.lu/en/2018/03/warning-regarding-virtual-currencies/.
11. 'Warning regarding Initial Coin Offerings and Tokens' (*Commission de Surveillance du Secteur Financier*, 14 March 2018) https://www.cssf.lu/en/2018/03/warning-regarding-initial-coin-offerings-icos-and-tokens/.
12. *Ibid*.
13. 'Statement' (*ESMA*, 13 November 2017) https://www.esma.europa.eu/sites/default/files/library/esma50-157-828_ico_statement_firms.pdf.
14. 'Advice on Initial Coin Offerings and Crypto-Assets' (*ESMA*, 9 January 2019) https://www.esma.europa.eu/sites/default/files/library/esma50-157-1391_crypto_advice.pdf.
15. Regulation (EU) 2017/1129 of the European Parliament and of the Council of 14 June 2017 on the prospectus to be published when securities are offered to the public or admitted to trading on a regulated market [2017] OJ L68/12, Article 1(3).

16. *Administration des contributions directes*, Circular L.I.R. No. 14/5 – 99/3 – 99*bis*/3 2018.
17. *Administration de l'enregistrement, des domaines et de la TVA*, Circular No. 787 2018.
18. Law of 12 November 2004 on the fight against money laundering and terrorist financing transposing Directive 2001/97/EC of the European Parliament and of the Council of 4 December 2001 amending Council Directive 91/308/EEC on prevention of the use of the financial system for the purpose of money laundering.
19. *Ibid*.
20. *Ibid*., Article 7-1.
21. 'ML/TF Vertical Risk Assessment: Virtual Asset Service Providers' (*Luxembourg Ministry of Justice*, December 2020) https://mj.gouvernement.lu/dam-assets/dossiers/blanchiment/ML-TF-vertical-risk-assessment-on-VASPs.pdf.
22. Aaron Grunwald, 'First blockchain property tokens issued in Lux' (*Delano*, 24 July 2019) https://delano.lu/article/delano_first-blockchain-property-tokens-issued-lux.
23. 'Financial Innovation: a challenge and an ambition for the CSSF' (*Commission de Surveillance du Secteur Financier*, 8 February 2021) https://www.cssf.lu/wp-content/uploads/C_Financial-innovation_February-2021.pdf.
24. 'Submission of a concrete project' (*Commission de Surveillance du Secteur Financier*) https://www.cssf.lu/wp-content/uploads/Innovation_Hub_Project_en.docx.
25. 'Blockchain and distributed ledgers, national technical standardisation report' (*Institut Luxembourgeois de la Normalisation, de l'Accréditation, de la Sécurité et Qualité des Produits et Services*, June 2021) https://portail-qualite.public.lu/dam-assets/publications/normalisation/2021/ilnas-national-technical-standardization-report-blockchain-and-dlt.pdf.
26. Law of 6 April 2013 on dematerialised securities, Article 1(11).
27. *Projet de loi 7363 portant modification de la loi modifiée du 1er août 2001 concernant la circulation de titres*.

* * *

Acknowledgment

The authors wish to acknowledge the valuable contribution of Sonia Vanzo to this chapter. Sonia works in the financial institutions department of Eversheds Sutherland (Luxembourg) LLP and specialises in investment funds. Sonia holds an LL.M. in Commercial and Corporate Law from Erasmus University Rotterdam and an LL.B. in European Law from Maastricht University (the Netherlands).

José Pascual
Tel: +352 278 64695 / Email: josepascual@eversheds-sutherland.com

José Pascual is the managing partner of Eversheds Sutherland (Luxembourg) LLP and specialises in regulatory matters and investment funds formation work, advising domestic and foreign clients on matters relating to the structuring, setting up and organisation of alternative investment funds (whether regulated or non-regulated) as well as on UCITS. This includes contracts, company law, regulatory matters and operating arrangements, with a specific focus on private equity funds, real estate funds, infrastructure funds, hedge funds, debt funds and any other type of alternative assets funds, as well as the related acquisition structures. He is also deeply involved in the corporate and transactional aspects relating to such alternative funds and the structures set up for acquisition purposes.

José holds a postgraduate degree (*Mastère Spécialisé*) from the École des Hautes Études Commerciales (HEC), Paris in partnership with the École Supérieure de Commerce de Paris (ESCP) (France), and a Master's degree from the Universidad Complutense de Madrid in partnership with the Diplomatic School of Spain, Madrid (Spain).

José is an active member of various working committees at the Association of the Luxembourg Fund Industry (ALFI).

Bernard Elslander
Tel: +352 278 64690 / Email: bernardelslander@eversheds-sutherland.com

Bernard Elslander is a principal associate in the financial institutions department of Eversheds Sutherland (Luxembourg) LLP and specialises in investment funds law, advising international clients such as private equity and real estate portfolio managers on the structuring, formation, management and obligations of Luxembourg regulated and unregulated vehicles with a particular focus on alternative investment vehicles.

Prior to joining Eversheds Sutherland, Bernard gained experience in a number of top tier international law firms and consulting companies both in Belgium and in Luxembourg.

Bernard was admitted to the Brussels Bar in 2005 and to the Luxembourg Bar in 2014, and graduated with an LL.M. from Durham University (UK) and a Master of Laws from the Catholic University of Louvain (Belgium).

Clément Petit
Tel: +352 278 64683 / Email: clementpetit@eversheds-sutherland.com

Clément Petit is an associate in the financial institutions department of Eversheds Sutherland (Luxembourg) LLP and specialises in regulated and non-regulated investment funds with a focus on UCITS, as well as alternative investment funds and AIF managers under the Alternative Investment Fund Managers Directive (AIFMD). In addition, he worked as secondee in an international Swiss bank on the acquisition of another Luxembourg-based bank and as an AIF manager on AML/CFT aspects. Clément was admitted to the Luxembourg Bar in October 2018 and holds a Master's degree from the Nancy Faculty of Law (France) and an LL.M. degree from Swansea University (Wales).

Eversheds Sutherland LLP

The Marivaux, 33, Rue Sainte Zithe, L-2763, Luxembourg
Tel: +352 278 64700 / URL: www.eversheds-sutherland.com

Mexico

Carlos Valderrama, Diego Montes Serralde &
Evangelina Rodriguez Machado
Legal Paradox®

Government attitude and definition

Since the enactment of the Law to regulate Financial Technology Institutions ("Fintech Law") on March 9, 2018, the Mexican Fintech and Cryptocurrencies Market has been evolving.

In March 2019, the Mexican Financial System Stability Council (composed of the Ministry of Finance and Public Credit, the Mexican Central Bank, the National Banking and Securities Commission, the National Insurance and Bonding Commission, the National Retirement Savings System Commission and the Bank Savings Protection Institute) decided to adopt a conservative stance regarding cryptocurrencies (defined as virtual assets in the Fintech Law), considering that there should be a healthy distance between virtual assets and the Mexican financial system.

The most recent communication dated June 28, 2021 from the main financial regulators (i.e. the National Banking and Securities Commission, the Ministry of Finance and Public Credit and the Mexican Central Bank), regarding operations with virtual assets, established that: (i) virtual assets do not constitute legal tender in Mexico nor are they currencies under the current legal framework; (ii) financial institutions with prior authorisation from the Mexican Central Bank may only enter into transactions with virtual assets corresponding to those activities carried out internally in order to carry out the transactions and services that such institutions enter into with their clients, or which they themselves carry out for their own account; and (iii) financial institutions are not allowed to enter into or offer to the public transactions in virtual assets, such as Bitcoin, Ether, XRP, etc., including deposits or any other form of custody, exchange or transmission.

Furthermore, the communication also described the stance of financial regulators towards so-called "stablecoins", establishing that the issuance of these collection rights against the issuer is not distinct from the activity of collection of resources, which is restricted to domestically regulated financial institutions. If it is decided that the technological infrastructure will be used to offer these issuance services, the corresponding authorisation by law must be obtained, as well as authorisation from the Mexican Central Bank to use these assets in the internal operations of the institutions.

Consequently, if the corresponding authorisations are not in place, no individual or legal entity is allowed to raise funds through the issuance or offer in the national territory of the instruments known as "stablecoins".

With respect to the legal definition of a virtual asset, the Fintech Law defines it as "*the representation of value electronically recorded and used among the public as a payment method for any kind of legal act and whose transfer can only be carried out through electronic means*". Notwithstanding the foregoing, the same law sets forth that in no case

shall virtual assets be understood as currency of legal tender on national territory, foreign currency or any other asset denominated in legal tender or in foreign currency.

In this regard, the following comments are made to clarify the scope of the law:

1. The Fintech Law only provides the legal framework for financial entities (Fintech institutions and banks) to perform operations with virtual assets.
2. The Mexican Central Bank is legally entitled to determine in secondary regulation the characteristics that virtual assets must fulfil to be used by financial entities.

Notwithstanding the above, financial authorities have also expressed that it is important to allow the admission of new technologies. An example of this includes the closing remarks of Mr. Alejandro Díaz de León, Governor of Banxico, which set forth that the main question is not whether to adopt them or not, but rather to identify the most convenient solution, when talking about central bank digital currencies before the Bank for International Settlements' Committee on Payments and Market Infrastructures. In this context, the Regulatory Sandbox will be an important tool to foster the emergence of new business models that operate with cryptocurrencies or blockchain technology.

Moreover, operation with virtual assets by non-financial entities is allowed in accordance with the terms listed in the Federal Law for the Prevention and Identification of Operations with Resources of Illegal Proceeds ("LFPIORPI") (see below for more details).

Finally, as of the date of preparation of this chapter, there are no virtual assets supported by either the Mexican Government or by Banxico.

Cryptocurrency regulation

The Fintech Law provides the main legal framework for financial entities to operate with virtual assets. However, this law also regulates several important components and entities that promote innovation within the Mexican financial system:

1. It creates two financial entities known as financial technology institutions ("ITFs"):
    a. Electronic payment funds institutions or wallets whose purpose is the issuance, administration, redemption, and transmission of electronic money for payments or transfers of funds.
    b. Collective financing institutions or crowdfunding whose purpose is to facilitate communication between applicants and investors so that the latter can provide resources to the former for specific projects. The law regulates both lending and equity activities.
2. Virtual assets: according to the Fintech Law, both ITFs and banks may perform operations using virtual assets, prior to recognition and authorisation from the Mexican Central Bank.
3. Innovative models (also known as Regulatory Sandboxes): these authorisations allow both financial and non-financial entities to carry out regulated activities using innovative technological models or means with different modalities from those currently existing in the Mexican market and with a lower regulatory burden (see below for more details).
4. Application programming interface: this tool allows financial entities to share information between them or with third parties to improve the customer's experience. This will give rise to the model known as "open finance", as opposed to the traditional model of "open banking".

In addition, the legal framework for virtual assets also includes the secondary provisions issued by the Mexican Central Bank known as "Circular 4/2019", whose main purpose is to determine the characteristics that virtual assets must fulfil in order to be used between financial entities (ITFs and banks) and their customers.

Nevertheless, as of July 2021, Banxico has not determined any virtual assets that can be used under these conditions within the Mexican financial system. However, these financial entities can use the technology on which virtual assets are based in accordance with the terms listed in Circular 4/2019.

Finally, the legal framework for virtual assets also includes the LFPIORPI. This law regulates operations with virtual assets performed by non-financial entities with a specific scope for the prevention of money laundering and terrorism financing. This law considers operations with virtual assets as vulnerable activities (designated non-financial businesses and professions for Financial Action Task Force purposes).

Sales regulation

In Mexico, there are no official categorisations other than the definition of virtual assets as a "*representation of value electronically recorded and used among the public as a payment method for any kind of legal act and whose transfer can only be carried out through electronic means*" set forth in the Fintech Law. The only mention of a different type of crypto asset was made by the Ministry of Finance and Public Credit, the National Banking and Securities Commission and the Mexican Central Bank in a joint communication in which they determined their position towards stablecoins.

On the other hand, the use of virtual assets is regulated by the Fintech Law and by LFPIORPI regulations, but there are other tokens, such as stablecoins, that do not fulfil the requirements to be considered virtual assets pursuant to the Fintech Law. In this context, it is important to analyse whether the asset has the qualities of a security under the Mexican Securities Market regulatory framework, in which case that framework will be applicable.

Taxation

As of the date of preparation of this chapter, there is no specific tax regulation issued for cryptocurrencies; therefore, the corresponding tax impact must be analysed on a case-by-case basis.

In general terms, all persons in Mexico – whether individuals or companies – are obliged to contribute to public expenses, in accordance with the respective laws. There are several federal contributions that must be considered when making an investment in our country, among which are income tax and value-added tax ("VAT").

Income tax is a direct contribution levied on income received by residents in Mexico and residents abroad with or without a permanent establishment in the country. This tax is calculated by applying a rate of 30% to the taxable base determined in accordance with the parameters of the law. In the case of residents abroad without an establishment in Mexico, the tax is generally paid by means of a withholding.

The legislation governing this tax sets forth cases of accumulation of income, deductions from income, as well as schemes that, depending on the operation, have special characteristics.

VAT, as an indirect tax, is levied on the consumption of goods and services under various headings, such as the sale of goods, the provision of services, the granting of temporary use or enjoyment of goods and the importation of merchandise. This tax is currently levied at a general rate of 16% on the values established for calculating the tax in each case. This tax is caused by the person who disposes of goods, provides services or grants the temporary use or enjoyment of goods, and must transfer it and collect it from the person who acquires the good or service, or the lease, as the case may be.

It is also relevant to note that one of the most important attributes for both taxes is the residence of the active subjects, as it links them to the jurisdiction of the State that exercises its taxing power. In Mexico, tax residents are legal entities that have established in the country the main administration of their business, and individuals, as a general rule, who establish their home in Mexico or are nationals of the country, although this must be analysed on a case-by-case basis to determine such tax residence.

A final point to consider is the tax regime aimed at digital platforms recently in operation (June 2020), which applies to persons who obtain income from providing services or selling goods through digital platforms.

This tax regime is called: "*On income from the sale of goods or the provision of services through the internet, by means of technological platforms, computer applications and the like.*" Basically, it is the digital platform that must make the income tax and VAT withholdings and it will be the same platform that will pay these withholdings directly to the Tax Administration Service ("SAT").

Money transmission laws and anti-money laundering requirements

The only permitted financial entities that can operate with virtual assets, prior to the authorisation of the Mexican Central Bank, are Fintech institutions and banks. In that regard, money transmitters are not permitted to operate with virtual assets unless they are authorised to do so due to a temporary authorisation granted by the financial regulators under the Regulatory Sandbox regime.

On the other hand, regarding AML requirements applicable to transactions with virtual assets, it is important to distinguish who is the entity making those transactions: (i) Fintech institutions or banks; or (ii) other entities or natural persons.

For Fintech institutions and banks, there are specific KYC/AML rules for each financial entity and, for other entities and natural persons, the general rules of the LFPIORPI apply.

The obligations for Fintech institutions and banks are highly strict and have requirements such as the development of an AML prevention manual, the formation of internal structures in charge of the AML department, being the Compliance Officer and the Communication and Control Committee, and a risk-based approach analysis, among others.

The obligations for other entities and natural persons are more flexible, but they are subject to register before SAT to start uploading reports to the AML system provided by the Financial Intelligence Unit, and are also subject to report transactions that exceed a predetermined threshold of approximately USD 2,800 in one transaction or in the accumulated transactions of six months. For more information, please refer to the "Reporting requirements" section below.

Promotion and testing

The Fintech Law introduced the Regulatory Sandbox under the figure of "innovative models", which promotes new business models for financial and non-financial entities that use state-of-the-art technology, such as blockchain, or a novel way for providing financial services within the Mexican market.

The regulation in question implies a change in the regulatory paradigm in Mexico, as our financial law has its origin in Civil and Roman law, a system of codified laws that attempts to cover in an exhaustive way each area of application for the law that can generate legal consequences. Opposed to the above, the Mexican Regulatory Sandbox

is configured in such a way that it can even provide an *ad hoc* legal framework for these new business models.

The Regulatory Sandbox was introduced to provide a way for non-financial entities to carry out an activity reserved for financial entities authorised by the Mexican financial regulator using innovative technological tools or means or with different modalities from those existing in the Mexican market and to provide a safe space to carry out tests with financial services in a real, temporary, controlled environment and above all with less regulatory burden. This is achieved by obtaining temporary authorisation that will allow the applicant to offer financial services.

It is important to note that we recently had 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 Service programme, where Legal Paradox® acted as a sponsor, hand in hand with giants like 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 Rocio Haydee Robles Peiro, Fintech Law, context, content and implications, Mexico City, Mexico, *Tirant lo Blanch*.

Ownership and licensing requirements

There are no restrictions or licensing requirements for non-financial entities and natural persons on owning cryptocurrencies; they are only obliged to comply with the AML requirements set forth by the LFPIORPI. For more information, please refer to the "Reporting requirements" section below.

In that sense, the restrictions for owning cryptocurrencies are only directed to financial institutions. Fund managers and investment advisors are considered financial institutions pursuant to the Securities Market Law and the Investment Funds Law, so they are not entitled to operate with virtual assets under the Fintech Law. The only financial institutions entitled to operate with virtual assets are banks and Fintech institutions.

Investment advisors are persons who, without being Securities Market intermediaries, habitually and professionally provide portfolio management services by taking investment decisions in the name and on behalf of others, as well as habitually and professionally providing investment advice in securities, analysis, and issuance of investment recommendations on an individual basis. In this regard, if the crypto asset is not considered a virtual asset under the Fintech Law, it could be the case that the nature of that asset is a security pursuant to the Securities Market Law with which the investment advisor or the fund manager could operate.

Notwithstanding the above, the Investment Funds Law established that the assets subject to investment must be securities, titles and documents to which the regime of the Securities Market Law is applicable, registered in the National Securities Registry or listed in the International Quotation System.

Mining

There are no specific rules applicable to mining. However, in Mexico, a general principle applies: whatever is not prohibited by law is permitted for non-regulated people or businesses. Therefore, as there are no regulations or prohibitions applicable to mining, it is a permitted activity.

Notwithstanding the above, 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 has to meet the required levels of consumption or demand set by the Ministry of Energy pursuant to the Electric 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 cryptocurrency holdings.

However, it is important to mention that, from a fiscal perspective, our system is based on fiscal self-determination, as well as that certain reports are applicable from an AML regulatory perspective (see the "Reporting requirements" section below).

Reporting requirements

Reports issued by non-financial entities

The exchange of virtual assets made by non-financial entities in a habitual and professional way through electronic or digital platforms or the facilitation of buy and sell operations or specific, set means for transfer, custody or storage of such virtual assets is regulated by the LFPIORPI. This law provides that non-financial entities must inform the Ministry of Finance by means of the Financial Intelligence Unit when the amount of a transaction performed by a client is equal to or greater than 645 update and measurement units (approximately MXN 56,000, or USD 2,800, for 2021).

Reports issued by Fintech institutions

These reports are currently in force but inoperative, see "Cryptocurrency regulation" above for more details. However, according to the AML/CFT secondary regulation applicable to Fintech institutions, these entities must share a report with the Ministry of Finance (through the National Banking and Securities Commission) within the first 10 business days of each quarter when a client has traded virtual assets for legal tender or foreign currency and *vice versa*, as long as the amount of the transactions made in a quarter have been equal to or greater than 7,500 investment units (these are units of measurement that vary according to inflation and are determined periodically by the Mexican Central Bank) (as of July 15th, 2021, this amount was approximately MXN 51,400, or USD 2,571).

Reports issued by banks

These reports are currently in force but inoperative, see "Cryptocurrency regulation" above for more details. However, according to the AML/CFT secondary regulation applicable to banks, these entities must share a report with the Ministry of Finance (through the National Banking and Securities Commission) within the first 10 business days of each quarter when a client has: (1) bought a virtual asset using legal tender or foreign currency, no matter the amount of the transaction; and (2) sold a virtual asset in exchange for legal tender or foreign currency, as long as the amount of the transaction made has been equal to or greater than USD 2,250.

Estate planning and testamentary succession

There are no specific rules applicable to estate planning and testamentary succession for cryptocurrencies. Therefore, the general rules apply. It is important to highlight that the legal nature of virtual assets corresponds to intangible assets susceptible to appropriation.

In Mexico, inheritance is the transmission of all rights and obligations that are not extinguished by death. Inheritance is governed by the will of the testator or by the provisions of the law. In the first case we are dealing with a testamentary succession, and in the second, with a legitimate succession.

The ownership rights to cryptocurrencies of natural persons can be transferred on by legitimate succession or by testamentary succession. However, there are no legal specifications regarding a custodial exchange to designate a beneficiary of virtual assets in case of death. Currently, within some custodial exchanges, the power is granted to designate heirs who will receive control and custody of the cryptocurrencies.

Currently, there are no specific obligations with respect to non-custodial exchanges or for decentralised exchanges. The owner of the cryptocurrencies must transfer the private keys of his wallet to the future heir.

In the absence of a specific legal provision applicable to the testamentary succession of the ownership of cryptocurrencies, the general rules of succession set forth in the Federal or State Civil Code will apply.

In contrast, for banks and Fintech institutions, the law provides that in the event of the user's death, the institution shall send the corresponding amount of money or electronic payment funds lying in the account of the deceased user to the designated beneficiaries. The user designates beneficiaries, expressly and in writing, as well as the percentages for each of them, and the electronic payment funds could be also referred to virtual assets with the corresponding authorisation of the Mexican Central Bank.

Carlos Valderrama
Tel: +52 1 416 690 48 / Email: carlos@legalparadox.com

Carlos is the founder and managing partner of Legal Paradox® with an LL.M., *summa cum laude*, with more than 15 years of experience, including expertise in lobbying Fintech and Blockchain Laws in LATAM, decentralised finance (DeFi), self-sovereign identity (SSI), regulatory sandboxes, stablecoins, wallets, crowdfunding, exchanges, broker-dealers, blockchain, KYC/AML rules, investment funds and smart contracts (including programming them in solidity and hyperledger). He provides advice to private and public entities such as the British Blockchain Association, as a member of its Advisory Board (2017–2021) and as Regional Adviser. He is chair of the legal working group of the 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. Carlos lectures on blockchain at universities in Mexico and Latin America such as Universidad Panamericana and ITAM, as well as training judges at the Mexican Federal Judicial Institute, and officials of the Mexican Central Bank.

Diego Montes Serralde
Tel: +52 1 416 690 48 / Email: diego@legalparadox.com

Diego is a junior associate at Legal Paradox® whose practice focuses on blockchain and digital assets, DeFi, self-sovereign identity, AML assessment, data protection assessment and technical research projects. He has worked on a variety of Fintech and financial projects, even Legal Paradox®'s own developments. He is currently a researcher for the Cambridge Centre for Alternative Finance on the Regulatory Innovation, Digital Assets and Global Benchmarking teams, working on different technical and regulatory global research, and he contributed directly to the Fintech Map, a development by Legal Paradox®, which identifies more than 752 institutions operating in the Mexican Fintech sector. Diego was the winner of the "Best Pitch" award for LawWithoutWalls, a legaltech competition held by the University of Miami, and he lectures on blockchain at universities and courses in Chile, Paraguay and Mexico and has published several posts on the firm's blog.

Evangelina Rodriguez Machado
Tel: +52 1 416 690 48 / Email: eva@legalparadox.com

Evangelina is a lawyer and future Master in Law and International Business from the Universidad Europea del Atlántico. She is an enthusiast of decentralised finance and portfolio management in cryptocurrency, as well as a financial advisor in blockchain technology innovation. She is currently a Program Manager at Blockchain Academy Chile of the LatAmTech Finance business group, and she is also a teacher, instructor and speaker in blockchain, legaltech and DeFi. Evangelina is a writer in Spanish and collaborator for BeInCrypto media, an advisor of corporate structures and private contracts of Argentine law, as well as a member of the Blockchain and Artificial Intelligence Room of the Institute in Justice Systems Management of the Faculty of Law and Social Sciences of the Catholic University of Córdoba, Argentina.

Legal Paradox®

Volcán 150, Floor 5, Lomas de Chapultepec, Mexico City, Z.C. 11910, Mexico
Tel: +52 1 416 690 48 / URL: www.legalparadox.com

Montenegro

Luka Veljović & Petar Vučinić
Moravčević Vojnović i Partneri AOD in cooperation with Schoenherr

Government attitude and definition

Governmental position

Neither the Central Bank of Montenegro ("**CBM**"), the Capital Markets Commission ("**CMC**") nor the Ministry of Finance and Social Welfare ("**MoF**") as the most competent State authorities, nor any other governmental bodies, have issued any position or policy papers regulating the use of cryptocurrencies in the country. However, in July 2021, the MoF decided to establish a Directorate for Blockchain and Cryptocurrencies, tasked with defining policy and establishing a legal and regulatory framework governing the mining and use of cryptocurrencies and blockchain technologies, as well as with removing regulatory and administrative barriers to the establishment and use of cryptocurrencies and blockchain technologies.

Montenegro is a candidate country for membership in the European Union ("**EU**") and is currently a frontrunner in the accession negotiations process. Furthermore, Montenegro also uses the Euro as its legal tender, despite the fact that the country is not a member of the Euro area. Given the country's strong desire to join the EU, the competent State authorities generally tend to adopt its legislation and align their official policies with the European *acquis communautaire* and the overall guidelines of the European institutions. Since the European Commission has recently released the Proposal for a Regulation of the European Parliament and of the Council on Markets in Crypto-assets dealing with the subject at hand, it can be expected that Montenegro will transpose the solutions contained therein once the document is adopted.

Currently, cryptocurrencies are not regarded as an official means of payment in Montenegro, although their possession and/or use is not explicitly prohibited.

The CBM, as the institution responsible for monetary policy and regulating the banking system, stated in a press release that virtual currencies are not a legal means of payment in Montenegro, and that any transactions facilitated through such currencies are performed at one's own risk. The CBM also confirmed that it does not have information on how many individuals and companies are issuing and managing these currencies, or how many transactions are being made in the country. According to the CBM, cryptocurrencies do not have any impact on the banking system in Montenegro and they are not perceived as a threat to the banking system.

The CBM does not adopt any firm position towards the legal nature of cryptocurrencies. In one brief statement, the Vice Governor of the CBM has expressed his personal opinion that cryptocurrencies are closer to electronic securities than to fiat currencies, primarily

due to the fact that they: (i) have limited function of means of payment; (ii) are not units of account; and (iii) do not store value. However, the possibility that cryptocurrencies might obtain those characteristics at some point has not been ruled out by the Vice Governor.

Definition

The 2019 amendments to the Montenegrin Prevention of Money Laundering and Financing of Terrorism Act (in Montenegrin: *Zakon o sprječavanju pranja novca i finansiranja terorizma*) ("**AML Act**") have introduced a definition of virtual currencies into the Montenegrin legal system. Virtual currencies are defined as digital representations of value that: (i) are not issued by the CBM or other public authority; (ii) are not necessarily attached to a conventional currency; (iii) are accepted by natural or legal persons as a means of exchange; and (iv) can be transferred, stored and traded electronically. Additionally, the Rulebook on Indicators for Recognizing Suspicious Clients and Transactions (in Montenegrin: *Pravilnik o indikatorima za prepoznavanje sumnjivih klijenata i transakcija*) ("**Rulebook**") explicitly lists some cryptocurrencies as virtual currencies (e.g. Bitcoin, Litecoin).

This definition is based on Directive (EU) 2018/843 of the European Parliament and of the Council dated 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 ("**Directive 2018/843**"). Interestingly, however, the Montenegrin legislator did not transpose one important part of the Directive providing that virtual currencies do not possess the legal status of currency or money.

Cryptocurrency regulation

Montenegrin legislation does not explicitly prohibit the use of cryptocurrencies, but neither does it provide a firm and comprehensive legal framework for their use. That being said, only some aspects of cryptocurrencies (relating to money transmission and anti-money laundering) have been regulated so far.

However, depending on the qualification of the legal nature of cryptocurrencies, i.e. to their subsumption into categories of money, financial instruments or some other types of assets, regulation applicable to those instruments/assets may also be applicable to cryptocurrencies. Nonetheless, due to the apparent lack of relevant business practices and/or applicable case law, the potential application of legal regimes concerning other financial instruments/assets to cryptocurrencies is still to be tested in Montenegro.

Sales regulation

There is no legislation regarding the sale of Bitcoins or other tokens in Montenegro.

Taxation

Cryptocurrencies are not subject to special tax law procedures in Montenegro. Accordingly, Montenegrin tax rules do not include any special tax rules for income, profits or gains arising from transactions involving cryptocurrencies. Furthermore, the Tax and Customs Administration of Montenegro ("**Tax Authority**") has not issued any official opinions on the tax regime applicable to certain transactions involving cryptocurrencies.

There have been several transactions concerning the purchase and sale of immovable property in Montenegro performed through the use of cryptocurrencies as a means of payment (in particular, Bitcoins). However, those contracts have also stated the property

price in Euros, alongside its value in cryptocurrencies. As a consequence, the Tax Authority calculated the applicable taxes on the property's value in Euros, and disregarded its value expressed in cryptocurrencies.

Money transmission laws and anti-money laundering requirements

The AML Act has transposed some of the solutions provided for in Directive 2018/843.

The AML Act explicitly provides for the detecting and prevention of money laundering and terrorist financing measures that all legal entities and natural persons engaging in activities related to the issuing and managing of virtual currencies, including those providing exchange services between virtual currencies and fiat currencies, need to comply with. The Rulebook also mentions the use of virtual currencies as terrorist financing indicators.

Promotion and testing

In 2020, the CMC, in cooperation with the MoF and the CBM, started considering the introduction of a blockchain and digital property market in Montenegro. Discussions have been held with the Chinese financial market authorities in this regard, but no significant progress has been made thus far.

Furthermore, the CMC approved the creation of a regulatory sandbox for two innovative ideas in providing financial services developed by Estonian companies: (i) testing and development of global clearing and settlement based on the distributed ledger technology network; as well as (ii) the digitisation and development of a tokenised multilateral trading platform.

Ownership and licensing requirements

In Montenegro, there are no restrictions on investment managers owning cryptocurrencies for investment purposes, nor are there any explicit licensing requirements imposed on someone who holds cryptocurrency as an investment advisor or fund manager. Nonetheless, the general licensing requirements imposed on investment advisors/fund managers in accordance with capital markets regulations are still applicable in this particular case.

Mining

The mining of Bitcoins and other cryptocurrencies is not regulated in Montenegro. Accordingly, it is not explicitly prohibited. The Constitution explicitly stipulates that everything not prohibited by it or by law is free. However, the complete lack of regulatory framework and supervision over mining activities in Montenegro could cause some problems to potential miners.

Border restrictions and declaration

There are no explicitly prescribed border restrictions, nor obligations to declare cryptocurrency holdings as such. However, depending on:

(i) the qualification of the legal nature of cryptocurrencies, i.e. to their subsumption into categories of money, financial instruments or some other type of assets; and
(ii) the qualification of transactions undertaken involving cryptocurrencies,

restrictions prescribed in the Law on Foreign Current and Capital Operations and other legislative acts may be applicable.

Reporting requirements

The AML Act prescribes the obligation of reporting all transactions exceeding the value of EUR 15,000, which also relates to transactions involving cryptocurrencies. In addition, depending on:

(i) the qualification of the legal nature of cryptocurrencies, i.e. to their subsumption into categories of money, financial instruments or some other type of assets; and
(ii) the qualification of transactions undertaken involving cryptocurrencies,

reporting requirements prescribed in the Law on Foreign Current and Capital Operations and relevant bylaws may be applicable.

Estate planning and testamentary succession

There is no legislation, nor applicable case law, confirming and explaining the use of cryptocurrencies for purposes of estate planning and testamentary succession in Montenegro.

Luka Veljović
Tel: +382 20 228 137 / Email: l.veljovic@schoenherr.me

Luka Veljović is an associate who has been working with Schoenherr since 2018. Based in the Montenegro office, he is a member of the corporate/commercial practice group, with a track record in real estate and construction, energy and regulatory law in Montenegro and the Western Balkans region. Some of the clients he has advised include Shanghai Electric Power, Enemalta plc, Rakita Exploration, EPCG, CGES, Ludwig Pfeiffer, United Group and Adient Automotive. Luka earned his LL.B. degree at the Faculty of Law, University of Montenegro, while spending part of his studies at the University of Maribor (Slovenia), the University of Zagreb (Croatia) and the University of Nice Sophia Antipolis (France). He is currently pursuing his LL.M. degree at KoGuan Law School, Shanghai Jiao Tong University.

Petar Vučinić
Tel: +382 20 228 137 / Email: p.vucinic@schoenherr.me

Petar Vučinić is an associate focusing mainly on banking, finance and capital markets, and dispute resolution. He was part of the team advising on the last two bond issuances of the State of Montenegro and also has extensive experience advising clients on OTC derivatives transactions under ISDA documentation. Also, Petar regularly advises clients in the financial services sector on regulatory matters. Petar graduated from the Faculty of Law of the University of Montenegro in Podgorica (LL.B. 2018) where he also obtained a specialist diploma in business law (2019). Petar is fluent in English and German alongside his native Montenegrin language.

Moravčević Vojnović i Partneri AOD
in cooperation with Schoenherr

Boulevard Džordža Vašingtona 98, The Capital Plaza, VIII floor, ME-81000 Podgorica, Montenegro
Tel: +382 20 228 137 / URL: www.schoenherr.eu

Netherlands

Gidget Brugman & Sarah Zadeh
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 Nederlandse 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]

Apart from the warnings and caution towards (services around) cryptocurrencies, DNB has a positive attitude towards introducing Central Bank Digital Currencies. DNB recently completed the initial exploratory phase, where it, among other things, conducted technical experiments with other central banks in the Eurozone. On 14 July 2021, DNB decided to go to the next phase, being that, over the next two years, 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, the Dutch Authority for the Financial Markets (*Autoriteit Financiële Markten*, "**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 Initial Coin Offerings ("**ICOs**").[8] Investing in ICOs does not differ in nature from participating in customary investment funds or Initial Public Offerings. 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.[9]

Following an investigation in December 2018 by DNB and AFM, 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).

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.[10] 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*."[11]

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).[12] 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.[13]

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 like 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**"), whilst other investment cryptos are structured in a way that prevents them from qualifying as such.[14] 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[15] 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.

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.

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*).[16]

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.[17] 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.[18] 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*).[19] However, when an individual actively pursues the growth of his assets, these may also be taxed in Box 1 (*income from other activities*).[20] In that case, income from assets is regarded differently to normal asset management.[21] 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%.[22]

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*).[23]

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.[24]

If a company is paid in cryptocurrencies for its services or supplies, it must convert the cryptocurrencies into fiat currency (Euros). 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.[25] The first bracket will be extended further in 2022 to a taxable income of up to €395,000.[26]

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.[27] 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.[28] Finally, mining as such is not subject to VAT, because the recipient of the mining services cannot be determined.[29]

Money transmission laws and anti-money laundering requirements

Money transmission laws

There are currently no regulations that explicitly prohibit the use or trading of cryptocurrencies 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[30] 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,[31] 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[32] 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[33] 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.

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 is still discussion on how to qualify crypto-currencies. Are they goods? Are they things or proprietary rights? If the latter, what kind?

On 14 February 2018, the District Court of Amsterdam considered that Bitcoin has all the characteristics of a "property right" (*vermogensrecht*), 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".

In the Netherlands, it is also possible to levy a prejudgment or executory attachment on Bitcoins (and most likely similar cryptocurrencies).

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.

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.[34]

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.[35]

As cryptocurrencies are (intangible) assets, they are subject to inheritance tax.[36] The rate depends on the value of the inheritance, including the value of the cryptocurrencies, and the relationship between the heirs and the deceased.[37]

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.[38]

* * *

Endnotes

1. Including tokens.
2. https://www.government.nl/documents/parliamentary-documents/2018/03/08/letter-from-minister-of-finance-providing-an-initial-assessment-of-developments-in-crypto currencies.
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. https://www.afm.nl/en/nieuws/2017/nov/risico-ico.
9. Article 5:3 Financial Supervision Act.
10. *Autoriteit Financiële Markten* and *De Nederlandse Bank*, "Cryptos: recommendations for a regulatory framework", December 2018, p. 9.
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 terrorism financing, and amending Directives 2009/138/EC and 2013/36/EU.
12. The UK Financial Conduct Authority (FCA) and the Swiss Financial Market Supervisory Authority (FINMA) use a similar categorisation.
13. *Autoriteit Financiële Markten* and *De Nederlandse Bank*, "Cryptos: recommendations for a regulatory framework", December 2018, p. 9.
14. The definition of a financial instrument is set out in article 1:1 Financial Supervision Act.
15. Implementation by the Markets in Financial Instruments Directive.
16. Article 5.2 Income Tax Act 2001.
17. *Brief van de Staatssecretaris van Financiën van 28 mei 2018*, 2018-0000082316.
18. E. toe Laer, "*Welke waarde moet ik aanhouden voor bitcoins in de aangifte inkomstenbelasting*?", *FD* 9 March 2018.

19. Article 5.3 Income Tax Act 2001.
20. Article 3.90 Income Tax Act 2001.
21. https://www.kvk.nl/informatiebank/belastingheffing-over-cryptocurrency-zoals-bitcoins/.
22. Article 2.10 Income Tax Act 2001.
23. Article 3.2 Income Tax Act 2001.
24. https://www.belastingdienst.nl/wps/wcm/connect/nl/werk-en-inkomen/content/cryptovaluta.
25. Article 22 Corporate Tax Act.
26. https://www.rijksoverheid.nl/onderwerpen/belastingplan/belastingwijzigingen-voor-ondernemers/vennootschapsbelasting.
27. CJEU 22 October 2015, C-264/14, *Hedqvist*; VAT guidelines para. 759.
28. CJEU 22 October 2015, C-264/14, *Hedqvist*; VAT guidelines para. 759.
29. CJEU 22 October 2015, C-264/14, *Hedqvist*; VAT guidelines para. 759.
30. Directive 2015/2366/EU of the European Parliament and of the Council of 25 November 2015 on payment services in the internal market, EU 2015/2366.
31. https://www.dnb.nl/media/cz3fjb4f/explanatory-notes-to-the-form-for-registration-as-a-crypto-service-provider.pdf.
32. (Co-)policymakers of the crypto asset service provider include persons actually (co-)determining the policy, management board members and supervisory board members.
33. Court of Rotterdam, 7 April 2021, ECLI: RBROT:2021:2968.
34. https://www.belastingdienst.nl/wps/wcm/connect/nl/bagage/content/geld-meenemen-op-reis.
35. 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)*", Universiteit Amsterdam, April 2021, p. 39.
36. L.A.G.M. van der Geld, "*De executeur in een nalatenschap met bitcoins en andere digitale bezittingen*", *Tijdschrift Erfrecht* 2014/6, p. 126.
37. https://www.belastingdienst.nl/wps/wcm/connect/nl/werk-en-inkomen/content/cryptovaluta.
38. 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)*", Universiteit Amsterdam, April 2021, p. 39.

Gidget Brugman
Tel: +31 20 5600 567 / Email: gidgetbrugman@eversheds-sutherland.com

Gidget is a partner in Eversheds Sutherland's Financial Services group. She advises financial institutions on a broad range of regulatory matters regarding the Dutch Act on Financial Supervision and the Dutch AML Act, such as issues of scope, licensing, passporting, customer due diligence, conduct of business rules, capital requirements, governance, fit and proper testing, the regulatory aspects of M&A/finance transactions, as well as on all documentation involved. Gidget has a special interest in payments, fintech (including banks, crypto assets and blockchain companies) and ESG (green fintech). She heads the Dutch blockchain and crypto assets working group within Eversheds Sutherland. Gidget also assists companies with financial litigation issues (duty of care, misrepresentation, cooperation agreements) and has extensive experience in class actions. She represents both claimants and defendants.

Gidget regularly writes articles, speaks at conferences, gives courses, and provides training for clients in relation to a wide variety of financial services regulatory matters. In the Netherlands, Gidget is a member of the advisory board of the Association of Credit Unions, of the Association for Finance Companies, and of Holland FinTech.

Sarah Zadeh
Tel: +31 10 2488 066 / Email: sarahzadeh@eversheds-sutherland.com

Sarah is an experienced associate at Eversheds Sutherland and specialises in data protection, data security, IT and privacy. Sarah has specific experience in advising on the handling of data security and cyber security incidents, assisting in and advising on IT-related projects, negotiating appropriate contractual provisions and protections, and advising on privacy and ethics in relation to the use of 'new technologies', such as artificial intelligence, internet of things and blockchain.

Sarah has been working for a large number of Dutch, European and international clients and has been seconded at three (multi)nationals, including a large datacentre group. She is known for her knowledge of IT. In 2020, Sarah completed the Oxford Artificial Intelligence Programme at Saïd Business School, University of Oxford.

Prior to working at Eversheds Sutherland, Sarah worked as legal counsel, charged with handling privacy compliance and IT. She is frequently invited to showcase her expertise at seminars and conferences, and regularly publishes on blockchain-related subjects, such as cryptocurrency regulations and legal issues regarding non-fungible tokens (NFTs).

Eversheds Sutherland

De Cuserstraat 91, 1081 CN Amsterdam, PO Box 7902, Netherlands
Tel: +31 20 5600 600 / URL: www.eversheds-sutherland.com

Norway

Ole Andenæs, Snorre Nordmo & Stina Tveiten
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, and growth has been especially strong over the past year, according to the Financial Market Report 2021 by the Norwegian government.[1] During the pandemic, Norwegian consumers have increasingly sought new savings and investment alternatives. Cryptocurrency has received a level of attention that very few other investment options have received.

A survey conducted by Arcane Research (a division of Norwegian investment company Arcane Crypto), in cooperation with EY, shows that 300,000 Norwegians (approximately 7 per cent of the total population) own cryptocurrency (2021).

Previous surveys by Menon Economics (2018) and Arcane Research (2019) indicated that 5 per cent and 4 per cent of all Norwegians owned Bitcoin or another cryptocurrency, respectively. This represents an increase of as much as 75 per cent since 2019 based on the 2021 survey.[2,3,4]

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**). NFTs have unique identification codes so that they can be separated from each other and not duplicated, and are used to verify originals of digital collectibles.

Government discussions have varied between whether to embrace or forbid 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 how decentralised platforms should be handled legally and fiscally. Uncertainties in connection with bookkeeping, reporting, and legal and tax classification contribute to risks that can and should be managed.

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.

However, the government has been positive to exploiting blockchain technology for future technological advantages and opportunities to stimulate new business models and markets – both in the private and public sector.

Moreover, it has been focused on that financial products and services that use decentralised finance (**DeFi**) can eliminate the need for centralised third parties, in addition to reducing brokerage costs and making financial services more accessible, the solutions can, in certain contexts, be more secure because they eliminate counterparty and settlement risk. However, the government has addressed the legal challenges in the intercept between the General Data Protection Regulation (**GDPR**) and blockchain technology.

Government programmes

The Norwegian government signed the European Blockchain Partnership in 2018, an initiative to develop EU/EEA strategy to build a blockchain infrastructure for public services. In the Norwegian government's strategy for cooperation with the EU (2018–2021), the government outlined the following in regard to legislative cooperation in Europe through the EU's Digital Market Strategy (page 15):

> "The use of artificial intelligence and new technology like blockchains are other areas of importance for Norway. The Government will work to ensure that strict requirements continue to be set for secure storage and use of personal data, in both the private and public sectors. The Government will also seek to cooperate closely with the EU on promoting consumer protection in the digital economy."[5]

The Central Bank of Norway (the **Central Bank**) recently reported that Norwegians are using coins and bank notes for approximately 3–4 per cent of their financial transactions. This makes Norway the most cashless society in the world.[6] 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 of whether to introduce a central bank digital currency (**CBDC**), which is widely available electronic money issued by a central bank in the official monetary unit.

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 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.[7]

It has been an ongoing discussion in Norway whether banks and national currencies will be marginalised in a few years by global technology giants and cryptocurrencies. The question has so far been answered negatively by the Central Bank and other actors in the financial industry. This has mostly been rationalised based on the need for financial stability and efficient payment services. The payment market, however, is changing rapidly, platforms are becoming more and more user-friendly and cryptocurrencies that offer a stable value against a single currency or a basket of currencies could, in isolation, make cryptocurrency more attractive as a payment solution.

Commercial adaptation

Norwegian crypto companies provide services such as: (i) cryptocurrency payment technology; (ii) crypto and digital asset liquidity provisions; (iii) interbank trading platforms; (iv) crypto-fiat exchange, custody and brokerage services (both retail and institutional); and (v) crypto hedge funds. There are currently 10 entities registered with FSAN to provide exchange and storage of cryptocurrency in Norway.

While the Norwegian oil fund has an indirect Bitcoin holding through ownership in MicroStrategy, Tesla and Square, the fund is not currently holding any direct investments in virtual currency.[8]

At the time of writing, no crypto companies are listed on the Oslo Stock Exchange. However, Seetee AS, a fully owned subsidiary of Aker ASA, has invested approximately NOK 500 million in Bitcoin.[9] Furthermore, Arcane Crypto was listed on Nasdaq Stockholm in January 2021. Arcane Crypto develops and invests in projects focused on Bitcoin and digital assets, and currently holds various parts of the crypto-ecosystems of eight different portfolio companies, including brokerage, custody, marketplaces and software solutions.

We have observed that cryptocurrency has been used in order for large companies, such as Norwegian Air Shuttle (**NAS**), to reduce costs. Norwegian Block Exchange (**NBX**) started as a spin-off from NAS to introduce cryptocurrency payments to the air industry with the incentive of reducing costs related to payments. NBX is a Norwegian cryptocurrency exchange, custodian and payment system. The company also plans to become the Nordic region's first crypto bank (with a bank licence), to launch "stablecoin" for the Norwegian krone, and aims to list the company on the Oslo Stock Exchange in 2021.[10] NBX is the only exchange in the Nordics that offers insurance for its clients by being a part of Ledger Vault's insurance pool.[11]

One of the government's main concerns is blockchains being exposed to attacks that threaten integrity. In addition to the risk of losses related to technical vulnerabilities, there is also legal uncertainty associated with liability for such weaknesses. In addition to the lack of robust security and risk mitigation affecting individuals, it has been an opinion that DeFi could pose a risk to society more generally. Like traditional cryptocurrencies, decentralised platforms can be used for criminal activities, such as money laundering, hackers stealing investors' coins, scams and fraud. In a risk assessment, the Norwegian Police Security Service has concluded that the nature of cryptocurrencies is such that it is "very likely" that marketplaces for cryptocurrencies will be used for money laundering.[12]

One of the most discussed subjects is the Tax Administration's concern that companies and/or individuals may not report owning, selling, buying and mining cryptocurrencies to Norwegian authorities, combined with the difficulties for tax authorities to track cryptocurrencies. During the last couple of years, tens of thousands of individuals have been identified who have not reported their virtual wealth and income for taxation.

Blockchain technology

As discussed, 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 March 2018, Deloitte provided a study on behalf of the Ministry of Local Government and Modernisation on the potential of and barriers to using blockchain technology in the Norwegian public sector. According to the report, the main obstacle for the use of blockchain technology in the public sector is the absence of proof of concept. However, it was recognised that the opportunities for using blockchain technology can be both profitable and efficient. Furthermore, it was concluded that blockchains are not in conflict with current regulations, as long as the technology is not used for hidden value transfers.[13]

In Norway, several projects have commenced involving blockchain technology among private and public actors. For example, Det Norske Veritas (**DNV**) 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.[14]

Furthermore, projects using blockchain technology have been initiated in combination with sustainable climate projects aiming to influence greener consumer behaviour. One example is Empower, which has developed a Norwegian plastic exchange scheme (ecosystem) that includes a deposit system for the recycling of plastic waste, generating revenue for those involved in the clean-up. By using blockchain technology, each step of the process is tracked, from collecting plastic at the source through to the sorting process to its eventual recycling and reintegration back into the supply chain.[15] Especially following the latest UN report on climate change in 2021, it is interesting to comprehend whether the use of blockchain technology will be one of several measures to stimulate climate action.

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, 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, loan applicants who have acquired equity through investments experience, e.g., that their loan applications are rejected because the banks cannot rule out that the cryptocurrency has been used for money laundering or the financing of terrorist activities.[16]

Norway's largest bank, DNB, joined the Marco Polo Network in 2018, a trade finance platform aiming to provide the next generation in trade finance solutions by using blockchain technology.[17]

The Ministry of Finance stated in the Financial Market Report 2021 that the authorities follow developments within DiFi more generally, and that DeFi can potentially have a major impact on the financial system and the ability to control the flow of services. The Ministry aims to return to this in next year's Financial Market Report.[18]

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 European Union; 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, and EU legislation, such as, e.g., the Payment Services Directive 2, must be incorporated into the EEA Agreement and subsequently be transposed into Norwegian law by the Norwegian parliament (the lawmaker).

From a Norwegian perspective, it will most likely be of great significance how the EU and other European countries choose to regulate cryptocurrency.

In Norway, the Securities Trading Act, the Anti-Money Laundering Act (**AML Act**) and the Financial Undertakings Act regulate payment, investment and utility tokens.

Providers of exchange services and storage services for virtual currency are covered by the requirements of the AML Act *cf.* the Anti-Money Laundering Regulations (**AML**

Regulations) (implementing Directive (EU) 2018/843 – the Fifth Anti-Money Laundering Directive) § 1-3. Such services can only operate after having been registered with FSAN, as further described below.

The European Securities and Markets Authority (**ESMA**) has stated that an initial coin offering (**ICO**) may fall outside the scope of the existing rules and regulations; however, where ICOs qualify as financial instruments (for instance, trading/marketing of financial instruments), relevant legislation applies if the firms involved in the ICO conduct regulated investment activities. As a result, the Prospectus Directive, the Markets in Financial Instruments Directive (**MiFID**) and the Alternative Investment Fund Managers Directive may apply to firms involved in ICOs.[19] The same principle applies to Norwegian regulation (based on EU legislation), meaning that investors must give consideration as to whether their activities constitute regulated activities.

The European Commission is considering a joint regulation of virtual assets (the Regulation of Markets in Crypto-assets, or **MiCA**), which are currently not covered by other EU regulations such as MiFID II or the e-Money Directive. MiCA expands the definition of what constitutes a virtual currency service provider, both beyond what follows from the AML Regulations today (in Norway and the EU), and beyond the standards of the Financial Action Task Force.

Personal data

The Norwegian Personal Data Act (2018), 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) which stakeholders are deemed to be responsible for any non-compliance with the GDPR; (iii) how individuals' rights may be protected; 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 grounds to process the personal data (e.g., legitimate interest of the owners/operators of blockchain to comply with legal obligations).

Registration obligation

The following actors must register with FSAN according to the AML Regulations: (i) a company registered in Norway; (ii) a company operating from Norway; or (iii) a company whose business is aimed at 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.[20]

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. The registration obligation therefore also includes service providers who currently operate without being registered in the Business Register, conduct business via a private account, operate through platforms (such as, e.g., LocalBitcoins.com), or who target the Norwegian market. It is the activity itself that is the basis for the registration obligation.

Sales regulation

Cryptocurrency is not in itself a financial instrument. Recommendations for the purchase and sale of cryptocurrencies are therefore not covered by the advisory rules in the Securities Act and are thus not subject to supervision by FSAN.

In contrast to regulated savings and investment products, there is no statutory consumer protection for buyers of cryptocurrencies in Norway. FSAN has made it clear that until regulations on investor protection, for example, 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,[21] as investment in Bitcoin, for example, is volatile.

In February 2021, the European Financial Supervisory Authorities ESMA, the EBA (the European Banking Authority) and EIOPA (the European Insurance and Occupational Pensions Authority) 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. FSAN supported the joint statement and published a national warning in February 2021.[22]

Furthermore, FSAN recently announced a press release (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.[23]

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.

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.[24]

The tax authorities have so far identified up to 70,000 people in Norway who own cryptocurrencies, but estimate that the actual number is much higher. In the 2019 tax return, however, fewer than 5,000 people reported their cryptocurrency balance and earnings from

cryptocurrency trades.[25] The estimates for 2020 are not ready yet; however, as mentioned, tax authorities are of the opinion that millions of kroner in tax have been withdrawn.

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 initial value and the initial value 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.[26]

In case of inheritance and gifts received from individuals paying tax in Norway, the heir or recipient of the gift inherits the testator/giver's input value in the assets, resulting in the potential taxable earnings from the trade of cryptocurrencies being calculated from the testator/giver's input value and not on the basis of the currency's value at the time the gift was received. As a result, the evaluation of earnings resulting from the trade and sale of cryptocurrencies will vary if inherited or given as a gift from an individual resident abroad or in Norway.

Valued-added tax (**VAT**)

The Court of Justice of the European Union ruled in C-264/14 (*Hedqvist*) 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. FSAN 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. 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.[27]

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 stablecoins intended for the general public where the issuer guarantees a nominal value will, in principle, fall within the definition of e-money.[28]

The European Commission considers that investment tokens and stablecoins in particular may qualify as financial instruments as defined in MiFID II and corresponding provisions in the Securities Trading Act regulating companies that offer services related to financial instruments and the trading venues where these instruments are traded. This means that depending on the character of the investment token, it might fall within the definition of a financial instrument *cf*. the Securities Trading Act § 2-2 (e.g., being either transferable securities, money market instruments and/or units in collective investment undertakings).

A security token represents an ownership stake in an asset, typically a company, and entitles its holder to a share of profits in the asset. As a result, security tokens advocate a steady return as a core value proposition, in contrast to other utility tokens such as Ethereum.[29]

The AML Act, implementing the EU's fourth AML Directive, entered into force in Norway on 15 October 2018. AML regulation applies to exchange services (between virtual currencies and fiat currencies) and custodian wallet providers and is regulated in the newly amended AML Regulations, implementing the EU's fifth AML Directive (in force from 1 July 2021). The changes resulted in a new paragraph 1 of § 1-3 of the Norwegian AML Regulations, clarifying that 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.[30]

The actors falling within the AML Regulations are, among other things, required to carry out customer measures and report suspicious transactions to the Norwegian National Authority for Investigation and Prosecution of Economic and Environmental Crime (Nw: *Økokrim*). As previously described, the players covered by the AML Regulations must register with FSAN. In 2019, FSAN started conducting suitability assessments (including police certificates) as part of the registration process.[31]

Promotion and testing

FSAN has established a "regulatory sandbox"[32] for the purpose of increasing innovation within the fintech industry in order to facilitate for new actors and increased competition. 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.

Blockchangers (in the process of rebranding to Symfoni) was founded as a digital core infrastructure where organisations can easily and securely create digital ecosystems for collaboration. The platform creates services for the government in order to use blockchain for realisation of the government's digitisation strategy.[33] The current project involves cooperation with the Brønnøysund Register Centre (the national register in Norway) and where Blockchangers acts as an adviser and gives lectures on blockchain and cryptocurrency for the Tax Administration, Statkraft and several other players. Furthermore, a project has been initiated to build a shareholder register on a blockchain for Norway's leading bank, DNB.[34] In addition, Blockchangers represents Norway in the OECD's Blockchain Experts Policy Advisory Board.[35]

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.

Other than the requirement to register with FSAN, there is no licence requirement for cryptocurrency providers under Norwegian jurisdiction. A provider may fall outside the regulations if (i) no permanent presence in Norway is established, and (ii) the Norwegian market is not specifically targeted (e.g., a Norwegian website allowing the purchase or redemption of tokens to Norwegian currency).

FSAN supervises whether actors offering cryptocurrency to the Norwegian market comply with registration requirements and the AML Regulations. It was recently announced that the largest cryptocurrency exchange in the world, Binance, has stopped trading and payment in Norwegian kroner. Furthermore, the company has dropped Norwegian websites and will no longer have an official communication channel in Norwegian after they received a formal inquiry from FSAN.[36]

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 10 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.

FSAN may reject applications that do not meet the requirements of the AML Act, or if the information that accompanies the registration request is incomplete. It is not permitted to start exchange or storage services for virtual currency until FSAN has made a positive decision on the registration. If the conditions for registration are no longer met, FSAN may revoke the registration.[37]

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.

Mining

There are 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.[38] At the time of writing, data facilities that consume more than 0.5 MW have a reduced electrical fee.[39]

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.

When importing assets or other valuables purchased with cryptocurrency into Norway, the Norwegian Declaration Act does not accept receipt of the transaction as proof of the assets' custom value.[40]

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.

Future regulations

In September 2020, the European Commission presented a proposal (MiCA) that is now being considered by the European Parliament and the Council (alongside the Digital Operational Resilience Act). The proposal is part of the so-called "Digital Finance Package", which seeks to support innovation and competition in digital finance, in combination with risk-reducing measures for consumers and investors. The purpose of the proposal is to create an EU framework for markets in crypto activity, digital tokens and distributed ledger technology for use in financial services and to secure financial stability.

MiCA will cover the following types of crypto values: (i) "utility tokens" (issued for non-financial purposes, to provide digital access to an application, resource or service); (ii) "asset reference tokens" (which aim to maintain a certain value of several fiat currencies/commodities/cryptocurrencies, or a mixture of such values, and then constitute a means of payment for the purchase of goods and services, and which can be stored); and (iii) "e-money tokens" (which constitute cryptocurrencies with a stable value based on only one fiat currency, and which seek to have the same function as e-money).

Items (ii) and (iii) above are variants of what are often referred to as "stablecoins" and the scope includes markets for financial instruments. Particular attention is paid to so-called "stack coins", which will be subject to a number of requirements, especially those that meet the condition of being "significant", due to the importance of financial stability.

Some of the proposed rules applicable for cryptocurrency services are:

- Requirements for licences/permits, including revocation of such, and requirements for reporting of cross-border activities.
- Requirements for good business practice, organisation, client resource management, complaint procedures, conflicts of interest and outsourcing.
- Requirements for specific types of services: wallet services; exchange platforms; exchange between crypto and fiat, as well as crypto to crypto; placement and execution of orders; execution of orders on behalf of third parties; and advice related to crypto values.

According to the proposal, services that are regulated can be offered in the form of cross-border activities (passporting). More detailed rules are also given on supervision and administrative sanctions. So-called "significant providers" of stablecoins are proposed to be subject to supervision by the EBA. Rules are also intended to prevent market abuse, including insider trading and market manipulation.[41]

The Norwegian government has stated that the proposal will be considered EEA-relevant, and the Ministry will consider Norwegian implementation when the regulations are finally adopted.[42] The players who will come under the new regulation according to the proposal are only partially subject to special rules today, in that the AML Regulations include providers of exchange services between virtual currency and official currency, and storage services for virtual currency. Other actors associated with virtual currency are not specifically regulated, and those that are defined as reporting entities under the AML Regulations are not subject to other obligations, such as requirements for capital, IT security, investor and consumer protection, etc. It is reasonable to assume that the rules offered in the proposal must be implemented in Norwegian law by reference.[43]

It is currently uncertain when the process in the EU will be finalised; however, the regulations will most likely be introduced within a three-to-four-year timeframe.

* * *

Endnotes

1. https://www.regjeringen.no/contentassets/01932e015f9d4a7792e19fab6ca901b9/no/pdfs/stm202020210031000dddpdfs.pdf.
2. https://kryptografen.no/2021/03/16/300-000-nordmenn-eier-kryptovaluta/.
3. https://kryptografen.no/2019/02/14/en-halv-million-nordmenn-vil-kjope-kryptovaluta/.
4. https://www.menon.no/hvem-eier-bitcoin/.
5. https://www.regjeringen.no/globalassets/departementene/ud/dokumenter/eu/eu_strategy.pdf.
6. https://www.numismaticnews.net/world-coins/norway-moves-cashless.
7. https://www.norges-bank.no/tema/finansiell-stabilitet/digitale-sentralbankpenger/.
8. https://www.dn.no/innlegg/bitcoin/kryptovaluta/blokkjedeteknologi/innlegg-oljefondet-kan-ikke-se-bort-fra-bitcoin/2-1-942455.
9. https://www.akerasa.com/nyheter/borsmeldinger/artikkel/36900-aker-asa-launches-seetee-to-invest-in-bitcoin-and-blockchain-technology.
10. https://e24.no/naeringsliv/i/2djVPr/kjos-boers-henter-skatteetatens-kryptosjef.
11. https://nbxsupport.zendesk.com/hc/en-us/articles/360052814671.
12. https://www.pst.no/alle-artikler/utgivelser/ny-nasjonal-risikovurdering-om-hvitvasking-og-terrorfinansiering-for-2020-nra-2020/.
13. https://www.regjeringen.no/contentassets/f5db1086d5324ec786f440afcb5cde52/blokkjeder_offentlig_sektor_deloitte.pdf.
14. https://www2.deloitte.com/no/no/pages/technology/articles/blockahin-sjomat-dnvgl.html.
15. https://www.empower.eco/.
16. https://www.dnb.no/dnbnyheter/no/samfunn/derfor-kan-kryptovaluta-vaere-problematisk-for-bankene.
17. https://www.marcopolonetwork.com/news/dnb-successfully-completes-test-of-trade-finance-platform-in-marco-polo/.
18. https://www.regjeringen.no/no/dokumenter/meld.-st.-31-20202021/id2845705/?q=bitcoin&ch=4#match_0.
19. https://www.esma.europa.eu/press-news/esma-news/esma-highlights-ico-risks-investors-and-firms.
20. https://www.finanstilsynet.no/konsesjon/virtuelle-valutatjenester/.
21. https://www.finanstilsynet.no/nyhetsarkiv/nyheter/2021/forbrukere-og-kryptovaluta/.
22. https://www.finanstilsynet.no/contentassets/c24dcc7bd0504a1d83b3c0fa7a7cee8f/esma-eba-og-eiopa-advarer-forbrukere-mot-risikoene-ved-kryptovalutaer.pdf.

23. https://www.finanstilsynet.no/nyhetsarkiv/nyheter/2021/finfluensere-og-forbrukervern/.
24. https://www.skatteetaten.no/en/business-and-organisation/reporting-and-industries/industries-special-regulations/internet/tax-and-vat-on-virtual-currencies/.
25. https://kommunikasjon.ntb.no/pressemelding/kryptovaluta-for-milliarder-av-kroner-rapporteres-i-skattemeldingen?publisherId=1726411&releaseId=17905875.
26. https://www.skatteetaten.no/en/person/taxes/get-the-taxes-right/shares-and-securities/about-shares-and-securities/digital-currency/defi/.
27. https://www.skatteetaten.no/en/business-and-organisation/reporting-and-industries/industries-special-regulations/internet/tax-and-vat-on-virtual-currencies/.
28. https://www.norges-bank.no/contentassets/8971421ae47b47a1be6576f17a415f5c/fi_finansiellinfrastruktur2020.pdf?v=05/19/2020110355&ft=.pdf&v=05/19/2020110355&ft=.pdf.
29. https://www.coindesk.com/business/2021/06/30/security-tokens-are-back-and-this-time-its-real/.
30. https://www.regjeringen.no/contentassets/56fe59758a8f41979c0b2979e2835410/horingsnotat-hvitvaskingsforskrift-2019-master-v11-endelig-2194816.pdf.
31. https://www.finanstilsynet.no/konsesjon/virtuelle-valutatjenester/.
32. https://www.finanstilsynet.no/tema/fintech/finanstilsynets-regulatoriske-sandkasse/.
33. https://www.blockchangers.com/.
34. https://www.digdir.no/media/1623/download.
35. https://www.oecd.org/daf/blockchain/OECD-Blockchain-Expert-Policy-Advisory-Board-List-of-Participants.pdf.
36. https://e24.no/teknologi/i/EaJjga/verdens-stoerste-kryptoboers-kutter-i-norge-etter-brev-fra-finanstilsynet.
37. https://www.finanstilsynet.no/konsesjon/virtuelle-valutatjenester/.
38. https://www.regjeringen.no/no/dokumenter/prop.-107-ls-20192020/id2702091/?q=elavgift%20bitcoin.
39. https://www.skatteetaten.no/bedrift-og-organisasjon/avgifter/saravgifter/om/elektrisk-kraft/.
40. https://www.toll.no/no/verktoy/regelverk/tollabc/7/7-10/.
41. https://www.europalov.no/rettsakt/europeisk-rammeverk-for-markeder-for-kryptoverdier/id-28355.
42. https://www.regjeringen.no/contentassets/01932e015f9d4a7792e19fab6ca901b9/no/pdfs/stm202020210031000dddpdfs.pdf.
43. https://www.regjeringen.no/no/sub/eos-notatbasen/notatene/2020/des/markeder-for-kryptoverdier/id2790910/.

* * *

Acknowledgment

The authors would like to thank Karoline Angell for her valuable contribution to this chapter. Karoline is an Associate at Wikborg Rein's Oslo office and is part of the firm's Capital Markets practice. She works mainly with asset management and financial regulatory matters.

Tel: +47 22 82 75 10 / Email: ang@wr.no

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 Specialist Counsel 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).

Stina Tveiten
Tel: +47 22 82 75 33 / Email: sti@wr.no

Stina Tveiten is an Associate at Wikborg Rein's Oslo office and is part of the firm's Capital Markets practice. She works mainly with asset management and financial regulatory matters.

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

Portugal

Filipe Lowndes Marques, Mariana Albuquerque &
Duarte Veríssimo dos Reis
Morais Leitão, Galvão Teles, Soares da Silva & Associados

Government attitude and definition

Blockchain technology in general, and cryptocurrencies in particular, are closely followed topics in the financial technology industry amongst the Portuguese government and the relevant regulatory authorities, along with prevailing fintech trends in other jurisdictions. Particularly in recent years, these technologies have been brought to public attention largely due to the increase in the value of Bitcoin, the rise in the number of initial coin offerings (ICOs) globally, and their market capitalisation. This focus is also driven by some significant developments that the Portuguese market has seen in recent years in this sector, most notably the rise of tech-based companies and the steady increase in the use of cryptocurrencies in the last decade.

The most recent institutional developments include the approval of Ministerial Resolution 29/2020, dated 5 March 2020, which sets the framework principles for the creation of a Portuguese regulatory sandbox, and the approval of Ministerial Resolution 31/2020, dated 5 March 2020, which establishes the Portuguese Digital Mission Structure, which sets the main goals of the Portuguese digital agenda. The envisaged Portuguese regulatory sandbox should be overarching to include any area where technology should be given a freer testing field and will be designated by the terminology "Technology Free Zones" (from the Portuguese expression *Zonas Livres Tecnológicas*), and will be promoted and coordinated within the Portuguese Digital Mission Structure.

Blockchain technology is slowly being implemented in a significant number of projects in early stages of development but is yet to have mainstream usage in private or public organisations. For these reasons, the government and regulatory authorities have been invested in studying blockchain technology and cryptocurrencies 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 cryptocurrency transactions and/or investing in cryptocurrencies. We note that, as further described below, both Banco de Portugal and the Portuguese government have already put in place some specific measures to regulate crypto-assets at some point, in line with the European regulatory framework, particularly regarding measures to protect against money laundering and/or terrorist financing (AMLFT).

For the purpose of this chapter, cryptocurrencies can be broadly defined along the European Central Bank's (ECB) definition – to which the Portuguese authorities have largely subscribed – as a "digital representation of value, not issued by a central bank, credit institution or e-money institution, which in some circumstances can be used as an alternative to money".[1] Other useful constructions have been developed by the European Securities

and Markets Authority (ESMA) in its advice on ICOs and crypto-assets (January 2019)[2] and in a study requested by the European Parliament's Special Committee on Financial Crimes, Tax Evasion and Tax Avoidance (June 2018).[3]

In Portugal, cryptocurrencies do not have legal tender status and thus do not qualify as fiat currency, nor are they treated as "money" (whether physical or scriptural) or, in principle, "electronic money". In this respect, the European Banking Authority (EBA) in its report of 9 January 2019[4] identified limited cases where cryptocurrencies can be considered "electronic money" as defined in Directive 2009/110/EC (EMD2), provided they match the criteria set in EMD2.

Nonetheless, cryptocurrencies are largely seen as an alternative payment method with a contractual nature that results from a private agreement between participants of cryptocurrency transactions, and with intrinsic characteristics that somewhat replicate some of the core traits of traditional money: 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 cryptocurrencies, including those that have successfully launched government-backed cryptocurrency, there is no public governmental proposal to provide legal backing to cryptocurrencies. Cryptocurrencies are thus not backed by the Portuguese government or Banco de Portugal (Portugal's central bank).

Cryptocurrencies can also be seen under a different light concerning their functionality. In this context, there has been recognition of other types of tokens, such as utility tokens and security tokens, commonly marketed through ICOs. These may be differentiated by their distinctive function, since the former are largely linked to consumption and the latter to investment. For this reason, they encompass or give rise to many other rights, including, among others, the right to receive a product or service or economic rights. In 2018, the Portuguese government actually issued a token – GOVTECH – which was used to cast votes by allocating those tokens to competing projects, thereby replicating investment choices, in a technological competition sponsored by the Portuguese government. The initiative was the first of its kind in Portugal and demonstrates the Portuguese government's willingness to apply the technology (although still in a risk-free setting).

In light of the above, these new technologies have inevitably drawn the attention of the relevant regulatory authorities, most notably Banco de Portugal, the Portuguese securities authority (*Comissão do Mercado de Valores Mobiliários*, or CMVM) and the Portuguese insurance and pension funds authority (*Autoridade de Supervisão de Seguros e Fundos de Pensões*, or ASF).

Banco de Portugal, in its capacity as both central bank and national competent authority for the supervision of credit and payment institutions, has shown a clear interest in cryptocurrencies, notably from the perspective of consumer/investor protection and has issued a number of public statements and warnings in relation to cryptocurrencies, in line with the regulatory practices of other central banks of the eurozone and European regulatory authorities, such as the ECB and the EBA. We highlight, *inter alia*, Banco de Portugal's publications that have included a warning focused on Bitcoin (November 2013), where it cited the ECB's study, Virtual Currency Schemes (October 2012) (in which the ECB noted that it would be closely monitoring this phenomenon with a view to studying any necessary regulatory responses),[5] and a warning to consumers regarding the potential risks in using cryptocurrencies (October 2014).[6] Banco de Portugal has since also created a dedicated page headed "Virtual Currencies" on its website, where it warns consumers on the one hand, and credit institutions, payment institutions and electronic money institutions on the other hand, of certain risks entailed in cryptocurrencies.

More significantly, Banco de Portugal has recently issued Notice No. 3/2021, of 24 April, in which it regulates the rather recent registration of virtual asset service providers (VASPs) that undertake their activity within the Portuguese territory, resulting from the transposition of Directive (EU) 2018/843, 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 into Portuguese law, notably to the Portuguese AMLFT framework, approved by Law No. 83/2017, of 18 August (Portuguese AML Law).

Meanwhile, the CMVM has published a warning to investors, in line with other European regulatory authorities such as ESMA, alerting them to the potential risks of ICOs in order to raise awareness of these risks (November 2017),[7] and has also issued a notice relating to a specific ICO for the issuance of Portuguese token Bityond (May 2018),[8] stating that it did not consider it a security and, accordingly, Bityond was not subject to the CMVM's supervision or compliance with securities laws. A notice has also been issued to alert consumers to the risks of cryptocurrency (e.g. Bitcoin, Ether and Ripple), notably inadequate information and lack of transparency (July 2018).[9]

On 23 July 2018, the CMVM issued a formal notice addressed to all entities involved in ICOs[10] 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. In this context, the CMVM noted that tokens can represent very 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, approved by Decree-Law No. 486/99, of 13 November, as amended.

Cryptocurrency regulation

At present, there are no specific laws or regulations that govern the issuance of cryptocurrencies (except the rules established in the Portuguese AML Law). Hence, cryptocurrencies are not prohibited, and investors are allowed to purchase, hold and sell these assets.

Nevertheless, on 10 March 2015, Banco de Portugal issued a recommendation, urging banks and other credit institutions, payment institutions and electronic money institutions, to abstain from buying, holding or selling virtual currency due to the risks associated with the use of virtual currency schemes identified by the EBA (the Bank of Portugal's Recommendation).[11]

In relation to other types of tokens in Portugal, the same can be said as there are also no specific regulations applicable to other forms of virtual tokens.

However, 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 ICO, token or related activity. In this regard, the laws applicable to tokens will vary greatly depending on the specific characteristics of each token.

Thus, from a legal framework perspective, the main concern when analysing an ICO and the respective tokens will be to determine whether the ICO represents a utility token or a security token.

ICOs that aim to offer tokens that represent rights and/or economic interests in a specific project's results, use of software, access to certain platforms or virtual communities or other goods or services, may hypothetically overlap with consumer matters and become subject to certain regulations regarding consumer protection.

ICOs that aim to offer 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, may potentially be qualified as securities and cross over to securities' intensively regulated world, becoming subject to existing securities regulations, most notably regulations applicable to public offerings of securities and/or securities trading venues. In this respect, it should be noted that subsequent to ESMA's position in November 2017 stating that ICOs qualifying as financial instruments may be subject to regulation under EU law,[12] as of 9 January 2019, ESMA has published advice on ICOs and crypto-assets.[13] Notably, under the heading "Regulatory implications when a crypto-asset qualifies as a financial instrument", ESMA provides advice on the potential application of, notably, the Prospectus Directive (Directive 2003/71/EC, as amended), the Transparency Directive (Directive 2013/50/EU), the Markets in Financial Instruments Directive (MiFID II) (Directive 2014/65/EU), the Market in Financial Instruments Regulation (Regulation (EU) No. 600/2014) and respective implementing acts, the Market Abuse and Short-Selling Regulation (Regulation (EU) No. 596/2014 and Regulation (EU) No. 236/2012), the Settlement Finality Directive (Directive 2009/44/EC), the Central Securities Depository Regulation (Regulation (EU) No. 909/2014), and the Alternative Investment Fund Managers (AIFM) Directive (Directive 2011/61/EU).

It is also worth noting that, within the context of the information published regarding Portuguese cryptocurrency Bityond, mentioned above, the CMVM has already publicly stated that a token that allows its users to (i) participate in surveys related to the development of an online platform, and (ii) further donate tokens to the online platform for the development of new tools, is not qualified as a financial instrument, i.e. is not a security token, and therefore is not subject to securities law or the supervision of the CMVM.

Additionally, in its formal notice addressed to entities involved in ICOs, dated 23 July 2018, and mentioned above, the CMVM clarified the elements that may, in abstract, implicate the qualification of security tokens as securities, namely: (i) if they may be considered documents (whether in dematerialised or physical form) 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 item, the CMVM will take into account any elements, including those made available to potential investors (which may include any information documents, e.g. 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: (a) to grant the right to any type of income (e.g. the right to receive earnings or interest); or (b) undertaking certain actions, by the issuer or a related entity, aimed at increasing the token's value.

The CMVM thus concludes that if a token is qualified as a security and the respective ICO is addressed to Portuguese investors, 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, should the ICO qualify as a public offering, the CMVM further clarifies that a prospectus should be drafted and submitted, along with any marketing materials for the ICO, to the

CMVM for approval, provided that no exemption applies in relation to the obligation to draw a prospectus. Lastly, in this notice, the CMVM also alerts that where a token does not qualify as a security, its issuer should avoid the use, including in the ICO's documentation, of any expressions that may be confused with expressions commonly used in the context of public offerings of securities, such as "investor", "investment", "secondary market" and "admission to trading".

Also, as mentioned above, for businesses transacting with crypto-assets, it is important to note that since the transposition of Directive (EU) 2018/843, 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 into the Portuguese AML Law, the following persons (whether natural or legal) will have to be registered with Banco de Portugal prior to commencing their activity in Portugal: (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 its customers, to hold, store and transfer virtual currencies).

Sales regulation

Considering the lack of exclusive regulation in relation to cryptocurrencies in Portugal, as described under "Cryptocurrency regulation" above, the purchase and sale of cryptocurrencies *per se* are also not specifically regulated.

However, to the extent that a 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, (i) consumer protection (including national laws that transposed, among others, Directive 2002/65/EC of the European Parliament and of the Council, of 23 September 2002, concerning the distance marketing of consumer financial services, Council Directive 93/13/EEC, of 5 April 1993, on unfair terms in consumer contracts, Directive 2000/31/EC of the European Parliament and of the Council, of 8 June 2000, on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market), and (ii) securities and financial markets (including national laws that transposed, among others, the Prospectus Directive, the Transparency Directive, MiFID II and the AIFM Directive), 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

Despite rumours, so far in Portugal, there is no specific regime that deals exclusively with the taxation of cryptocurrencies. Nonetheless, the Portuguese Tax Authority has published three official rulings in the context of certain requests for binding information relating to cryptocurrencies: one in the context of personal income tax (December 2016);[14] and the other two in the context of value-added tax (VAT) (January and July 2019).[15] In the absence

of other laws and regulations that may clarify the taxation regime of cryptocurrencies, these rulings have an important weight and will work as precedents in relation to how the Portuguese Tax Authority will look into cryptocurrency and cryptocurrency-related activities when interpreting existing tax provisions and deciding whether or not a certain fact or action should be subject to Portuguese tax (corporate, individual, VAT or stamp duty). In any event, as these were given in the context of requests for binding information, the Portuguese Tax Authority may revoke these rulings in the future.

In the 2016 official ruling, the Portuguese Tax Authority analysed the possible classification of cryptocurrencies within certain types of income that are subject to Portuguese tax, notably capital gains, capital income and income from business activities, and decided that, as a general rule, natural persons should not be taxed in respect of gains derived from the valuation or sale of cryptocurrencies, except that, in the case of sale of cryptocurrencies, if they correspond to the individual's main recurrent activity, income obtained from such activity could be subject to Portuguese tax. It should also be noted that this was only a partial decision that did not elaborate on other types of income derived from other cryptocurrency-related activities (e.g. mining and farming activities).

In the 2019 official rulings, the Portuguese Tax Authority confirmed the precedent from the Court of Justice of the European Union (Case C-264/14, *Skatteverket v. David Hedqvist*) to argue that although cryptocurrencies 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.

Money transmission laws and anti-money laundering requirements

As previously mentioned, the Portuguese AML Law[16] introduced a mandatory registration requirement for all VASPs that undertake their activity within the Portuguese territory. The registration procedure is to be established in accordance with article 112-A of the Portuguese AML Law and Banco de Portugal's Notice No. 3/2021, of 24 April 2021, which establish the obligation of: (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 its customers, to hold, store and transfer virtual currencies) to be registered prior to engaging in their activity.

The following entities are considered to operate within Portuguese territory: (a) Portuguese companies (incorporated in Portugal); (b) entities with permanent establishment in Portugal; and (c) entities that are obliged to open an activity with the Portuguese tax authorities. We further note that this understanding of what it means to "*operate within the Portuguese territory*" is not, however, expressly set out in the law, so there may be the risk that Banco de Portugal changes its view in the future.

Banco de Portugal has been the competent authority in registering and verifying compliance with the applicable legal and regulatory provisions governing the prevention of money laundering and terrorist financing by the abovementioned persons, being, as of this moment, according to the public list published by Banco de Portugal, three registered entities.

According to the Portuguese AML Law, as VASPs are now considered "obligated entities", the general undertaking of risk management in the use of new technologies or products

that are prone to favour anonymity is mandatory. This means that, under Portuguese law, VASPs are legally required to monitor, analyse and document the specific procedures to address any specific risks of money laundering and terrorist financing.

In addition, obliged entities must undertake identification procedures and customer due diligence whenever there is an occasional transaction of more than €15,000, as well as reinforce their identification procedures and customer due diligence when they identify an additional risk of money laundering or terrorist financing in business relationships, in occasional transactions or in the usual operations of the customer. Pursuant to the Portuguese AML Law, 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, whether for new products or existing ones. This has obvious implications for cryptocurrencies and cryptocurrency-related activities (including cryptocurrency exchanges) in case those operations intersect with the activities and operations of entities that are covered by obligations imposed by the Portuguese AML Law.

It should be made clear, however, that in relation to VASPs, Banco de Portugal's competence is limited to AMLFT issues and does not extend to prudential, behavioural or other areas of supervision.

Promotion and testing

The Portuguese 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. Now, with the publication of the Ministerial Resolutions referred to above and the creation of the Portuguese Digital Mission Structure, the launch of a Portuguese regulatory sandbox is closer to being achieved.

Additionally, both the CMVM and Banco de Portugal have specific spaces for fintech on their webpages, http://www.cmvm.pt/en/ and https://www.bportugal.pt/en/, respectively, which include, *inter alia*, information regarding distributed ledger technology, ICOs, and tokens.

These fintech spaces were created with the intent to facilitate the provision and exchange of information and dialogue between these regulators and developers or sponsors of new financial technologies that cross over with the areas of regulatory competence of the CMVM and Banco de Portugal, and also to clarify the regulatory framework applicable to the same. These objectives are obtained mainly by having a dedicated contact within the CMVM and Banco de Portugal that deals solely with issues relating to fintech, and by being active in promoting conferences and workshops aimed at investors and the public in general with a formative and educational goal.

In 2018, a non-profit organisation, Portugal Fintech, and Banco de Portugal, the CMVM and ASF, joined efforts to create "Portugal FinLab – where regulation meets innovation", 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 also manages the Portugal Fintech Report, which is an annual report that contains data regarding the Portuguese fintech ecosystem and its development, and the Fintech House, launched in January 2020, which is a fintech hub.

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 cryptocurrencies 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 the Portuguese territory are required to obtain prior registration with Banco de Portugal, as provided for in the Portuguese AML Law and in Banco de Portugal's Notice No. 3/2021, of 24 April 2021.

Furthermore, insofar as cryptocurrencies are not qualified as financial instruments, advisory services that are made exclusively in relation to, and the exclusive management of, cryptocurrency 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.

One thing to note is that, given the fact that these instruments are not yet mainstream for consumers, the overall regulatory uncertainty and even some regulatory pushback (e.g. the Bank of Portugal's Recommendation), underpinned by the already existing and overarching obligations applicable to the provision of investment services, it is not likely for the time being that traditional investment advisors, including, among others, credit institutions and fund managers, will recommend or invest in cryptocurrencies.

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 cryptocurrency holdings.

Reporting requirements

There is no standalone reporting obligation in case of cryptocurrency 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 cryptocurrencies 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 Portuguese tax authorities, 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 cryptocurrencies. Estate planning and testamentary succession must therefore be analysed on a case-by-case basis, considering all variables involved.

* * *

Endnotes

1. *Cf.* EUROPEAN CENTRAL BANK, Virtual currency schemes – a further analysis, February 2015, available at https://www.ecb.europa.eu/pub/pdf/other/virtualcurrency schemesen.pdf. See also the definition of virtual currency included in the fifth AML Directive (Directive (EU) 2018/843).
2. *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.
3. *Cf.* ROBBY HOUBEN, ALEXANDER SNYERS, "Cryptocurrencies and blockchain. Legal context and implications for financial crime, money laundering and tax evasion", study at the request of the European Parliament's Special Committee on Financial Crimes, Tax Evasion and Tax Avoidance, dated June 2018, available at http://www.europarl.europa.eu/cmsdata/150761/TAX3%20Study%20on%20cryptocurrencies%20and%20blockchain.pdf.
4. *Cf.* EUROPEAN BANKING AUTHORITY, EBA Report with advice for the European Commission on crypto-assets, 9 January 2019, available at https://eba.europa.eu/.
5. *Cf.* BANCO DE PORTUGAL's public statement regarding Bitcoin, dated 22 November 2013, available in Portuguese at https://www.bportugal.pt/comunicado/esclarecimento-do-banco-de-portugal-sobre-bitcoin.
6. *Cf.* BANCO DE PORTUGAL's warning regarding the risks associated with cryptocurrencies, dated 3 October 2014, available in Portuguese at https://www.bportugal.pt/comunicado/alerta-aos-consumidores-para-os-riscos-de-utilizacao-de-moedas-virtuais.
7. *Cf.* CMVM's warning regarding the risks associated with ICOs, dated 3 November 2017, available in English at http://www.cmvm.pt/en/Comunicados/Comunicados/Pages/20180119.aspx.
8. *Cf.* CMVM's notice regarding the cryptocurrency Bityond, dated 17 May 2018, available in Portuguese at http://www.cmvm.pt/pt/Comunicados/Comunicados/Pages/20180517a.aspx.
9. *Cf.* CMVM's notice regarding risks of "virtual currencies", dated 5 July 2018, available in Portuguese at http://www.cmvm.pt/pt/CMVM/CNSF/ConselhoNacional DeSupervisoresFinanceiros/Pages/20180705.aspx.
10. CMVM's notice addressed to all entities involved in ICOs, dated 23 July 2018, available in Portuguese at http://www.cmvm.pt/pt/Comunicados/Comunicados/Pages/20180723a.aspx?v=.
11. *Cf.* BANCO DE PORTUGAL's Circular Letter No. 11/2015/DPG, dated 10 March 2015, Recommendation relating to buying, holding and selling virtual currencies, available in Portuguese at https://www.bportugal.pt/sites/default/files/anexos/cartas-circulares/11-2015-dpg.pdf.
12. *Cf.* EUROPEAN SECURITIES AND MARKETS AUTHORITY, Statement "ESMA alerts firms involved in Initial Coin Offerings (ICOs) to the need to meet relevant

regulatory requirements", dated 13 November 2017, available at https://www.esma.europa.eu /sites/default/files/library/esma50-157-828_ico_statement_firms.pdf.

13. See endnote 2 above.
14. *Cf*. AUTORIDADE TRIBUTÁRIA E ADUANEIRA, Binding Information provided in process No. 5717/2015, dated 27 December 2016.
15. *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.
16. Law No. 83/2017, of 18 August, transposing Directives 2015/849/EU of the European Parliament and of the Council of 20 May, and 2016/2258/EU of the Council of 6 December.

* * *

Acknowledgment

The authors would like to thank Salvador Sampaio Fontes for his valuable contribution to this chapter. Salvador joined the firm in March 2020 and is a member of the banking and finance team.

Previously, Salvador attended an internship at the legal department of Banco Santander Totta (July 2018) and at the Bank of Portugal (2019). He also attended a short-term internship at Morais Leitão, Galvão Teles, Soares da Silva & Associados (August 2019).

Tel: +351 213 817 400 / Email: sfontes@mlgts.pt

Filipe Lowndes Marques
Tel: +351 213 817 400 / Email: flmarques@mlgts.pt

Filipe Lowndes Marques joined the firm in 2001. He is the coordinator of the banking and finance department and is a member of the firm's board of directors.

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.

His investment fund team was considered by *Chambers Europe* as "Portugal's top practice in investment funds".

Mariana Albuquerque
Tel: +351 213 817 400 / Email: msalbuquerque@mlgts.pt

Mariana Albuquerque joined the firm in 2014. She is a member of the banking and finance team and of Team Genesis.

She develops her work primarily in the area of banking and finance law, with a special focus on compliance by providing legal advice and consultancy with regard to the regulation and supervision of banks and other financial institutions, in securitisation transactions, negotiating derivatives and other financial instruments, in structured finance, corporate finance and project finance transactions and in negotiating the sale and purchase of non-performing loans portfolios.

She also works in debt restructurings, debt issues and other issues of hybrid financial instruments, having experience also in public offers and takeover bids. As a member of Team Genesis, Mariana works primarily with Fintech- and Regtech-related subjects.

Duarte Veríssimo dos Reis
Tel: +351 213 817 400 / Email: dvreis@mlgts.pt

Duarte Veríssimo dos Reis joined the firm in 2020. He is a member of the banking and finance team.

Duarte advises clients with respect to banking and finance law, with special focus on the regulation and supervision of banks and other financial institutions. Duarte also represents lenders and borrowers in secured lending transactions and provides legal advice in respect of real estate finance and debt issuances.

Before joining the firm, Duarte was a member of the banking and finance department of the Luxembourg office of Loyens & Loeff between 2018 and 2020, where he advised international clients with regard to leveraged finance, fund finance and secured lending transactions.

Morais Leitão, Galvão Teles, Soares da Silva & Associados

Rua Castilho, 165, 1070-050 Lisbon, Portugal
Tel: +351 213 817 400 / URL: www.mlgts.pt

Serbia

Bojan Rajić & Mina Mihaljčić
Moravčević Vojnović i Partneri AOD Beograd
in cooperation with Schoenherr

Government attitude and definition

The Serbian Parliament enacted the new Digital Assets Act ("**DAA**"), intended to regulate, but also enhance, the use of cryptocurrencies and similar instruments in Serbia. The application of the new legislation started from June 2021. For the first time, the DAA recognises and governs, among other things, digital asset issuance and trading in the Republic of Serbia, as well as provision of digital asset-related services. It further introduces the concepts of pledge over digital assets and fiduciary agreements for securing receivables or for other purposes, and allows and regulates digital asset crowdfunding.

The DAA regulates all digital assets regardless of the technology on which they are based. It defines a digital asset as a digital record of value that can be bought, sold, exchanged or transferred, and that can be used as a medium of exchange or for investment purposes.

The DAA recognises two types of digital assets:

(i) virtual currencies – defined as a type of digital asset that is not issued and whose value is not guaranteed by the central bank or other public authority, which is not necessarily tied to a legal tender and has no legal status of money or currency, but is accepted by individuals or legal persons as a means of exchange and can be bought, sold, exchanged, transmitted and stored electronically; and

(ii) digital tokens – defined as any intangible property right that, in digital form, represents one or more other property rights.

The National Bank of Serbia ("**NBS**") is the governmental authority with competence over virtual currencies, while the Serbian Securities Commission ("**SEC**") has competence over digital tokens. For example, the SEC issues licences for provision of digital asset services, carries out supervision and gives opinions on the application of the legislation. The DAA sets forth that the regulatory framework stipulated by the Serbian Capital Markets Act ("**CMA**") applies to digital assets that could be qualified as financial instruments. However, the DAA recognises that certain digital assets may have "features of the financial instruments". Such digital assets will not be subject to registration and other requirements under the CMA, if each of the following conditions are satisfied: (i) such digital assets do not have features of shares; (ii) such digital assets are not exchangeable for shares; and (iii) over a period of 12 months, the total value of the digital assets issued by a single issuer does not exceed the Serbian dinar equivalent of EUR 3,000,000.

Exclusion of Government liability

The DAA makes it explicit that the Republic of Serbia, the NBS, the SEC or any other authority will not in any way guarantee the value of digital assets and will not be liable for damage that may occur as a result of digital asset transactions. Providers of digital

asset-related services must inform the potential client of the risks related to digital assets, including the possibility of partial or total loss of digital assets, in advance of establishing a business relationship.

Accordingly, the DAA introduced a "white paper" – a document published during the issuance of digital assets in accordance with the DAA – containing information on issuers of digital assets, the digital assets themselves and the risks associated with them and which allows investors to make an informed investment decision. Such white paper may be approved by a competent authority (the NBS and/or the SEC), which provides additional legal certainty and simplifies advertisement.

Cryptocurrency regulation

The concept of cryptocurrencies is introduced and now regulated by the newly adopted DAA (please see "Government attitude and definition" above) and accompanying bylaws.

Sales regulation

Under the DAA, digital asset service providers are authorised to organise a platform, but they must be incorporated in Serbia and hold the appropriate NBS/SEC licences. All interested parties can trade on a platform.

The DAA provides secondary and over-the-counter ("**OTC**") trading with or without an intermediary and explicitly allows the use of smart contracts for secondary trading; however, there are restrictions in regard to advertisement of digital assets without an approved white paper.

Taxation

Recently, the Serbian Parliament has also adopted a set of amendments to tax regulations, thereby defining the tax status of digital assets. The most important amendments to the Tax Acts are the following:

- **Value-Added Tax Act** – Transactions with cryptocurrencies made in accordance with the DAA (transfers of cryptocurrencies and converting them into money) are added to the list of financial transactions exempt from VAT.
- **Corporate Income Tax Act** – Sale or other transfers of digital assets against consideration by legal entities are subject to capital gains tax at the rate of 15%.
- **Personal Income Tax Act** – The incomes earned by trading in cryptocurrencies are considered capital gains and are therefore taxed at the rate of 15%.
- **Property Tax Act** – Digital assets are subject to inheritance and gift tax at the rate of 2.5%, whereby the tax base is the market value of such digital asset at the moment inherited or gifted.

Money transmission laws and anti-money laundering requirements

In Serbia, anti-money laundering ("**AML**") is regulated by the Law on Prevention of Money Laundering and Terrorism Financing ("**AML Act**"). The AML Act, to a great extent, transposes the principles and rules of the AML Directive, as a part of Serbia's efforts to harmonise its laws with EU law.

The AML Act recognises digital asset service providers and regulates their obligations. A digital asset service provider must obtain data on all stakeholders with regard to the digital asset transaction, such as: (i) personal name; (ii) residence address or business seat; and (iii)

address of the digital asset used in the transaction, i.e. the corresponding unique code of the transaction with the digital asset. Pursuant to the risk assessment, a digital asset service provider can further verify the accuracy of the collected data. Also, the digital asset service provider has to perform verification procedures regarding the collected data.

Also, the Serbian Criminal Code (RS Official Gazette, nos 85/2005, 88/2005, 107/2005, 72/2009, 111/2009, 121/2012, 104/2013, 108/2014, 94/2016 and 35/2019) ("**Criminal Code**") sanctions the crime of money laundering. Namely, under the Criminal Code:

> "*The one who converts or transfers assets while aware that such assets originate from a criminal activity, with intent to conceal or misrepresent the unlawful origin of the assets, or conceals and misrepresents facts on the assets while aware that such assets originate from a criminal activity, or obtains, keeps or uses assets with the intent, at the moment of receiving, that such assets originate from a criminal activity, shall be punished by imprisonment of six months to five years and a fine.*"

The Serbian authorities believe that the term "asset" can be interpreted to include crypto-assets, so the Criminal Code regulates laundering of crypto-assets as a criminal activity as described.

Promotion and testing

According to the Smart Specialization Strategy, one of the key documents adopted by the Serbian Government for improving the innovation and research ecosystem, two regulatory sandboxes have already been introduced:

(i) the FinTech sandbox, where innovative payment solutions can be tested within a limited market without regular prior registration; and

(ii) the MedTech sandbox, where unregistered medical devices can be imported for research and development on a fast-track procedure, if the company is settled in one of the Science Technology Parks.

The Serbian Government intends to implement more sandbox frameworks in the fields where it is possible to test artificial intelligence.

Ownership and licensing requirements

A digital asset service provider must be incorporated in a form provided under the Serbian Companies Act (i.e. partnership, limited partnership, limited liability company, joint-stock company) and hold the appropriate licences issued by the NBS or the SEC. A digital asset service provider must be incorporated in any of the mentioned legal forms and be "truly" operational in Serbia.

Under the DAA, a digital asset service provider must have a minimum registered capital of EUR 20,000 to EUR 125,000, depending on the type of service it will be providing: (A) **EUR 20,000** for the following activities: (i) receiving, transferring and executing orders relating to the purchase and sale of digital assets on behalf of third parties; (ii) services for the purchase and sale of digital assets for cash and/or funds in the account and/or electronic money; (iii) digital asset exchange services for other digital assets; (iv) storage and administration of digital assets for the account of users of digital assets and related services; and (v) services related to the issuance, offer and sale of digital property, with the obligation to redeem it, or without such obligation; (B) **EUR 50,000** with regard to (i) digital asset acceptance/transfer services, and (ii) digital asset portfolio management; and (C) **EUR 125,000** with regard to organising a platform for trading digital assets.

The following documents must be submitted as part of the application process: (i) a list of services that a company intends to provide; (ii) company bylaws; (iii) an activities programme, describing in detail how the services will be provided; (iv) measures that a company will undertake with regard to AML; (v) organisational structure; (vi) information about individuals who have qualified ownership; (vii) evidence that the applicant has the required registered capital; and (viii) evidence that the applicant has paid all applicable fees. The provided list of the required registration documents is not exhaustive.

A legal entity or individual who intends to provide only advisory services related to digital assets is not required to hold a licence. Furthermore, a digital asset service provider may also provide advisory services.

Mining

The DAA recognises the concept of digital asset mining, but this area is excluded from the scope of the DAA and thus remains unregulated, as there are no rules that regulate under which conditions and how mining activities can be undertaken. It can hence be deduced that mining is currently permitted in Serbia. Also, no authority has yet assumed the mining of cryptocurrencies as falling under its (explicit) supervision.

However, the provisions of the DAA would apply on disposal of acquired assets through mining, either via service providers or on the OTC market.

Border restrictions and declaration

There are currently no border restrictions or obligations to declare cryptocurrency holdings under Serbian law.

Reporting requirements

The DAA sets forth that general financial reporting regulations apply to digital asset service providers. However, the DAA explicitly prescribes that a digital asset service provider whose annual transactions exceed RSD 220,000,000 (approx. EUR 1,870,000) must conduct an audit, regardless of the applicable financial reporting rules.

Also, it should be presumed that general AML rules may also be applicable to cryptocurrency and blockchain transactions, i.e. that certain AML requirements apply irrespective of the transaction being made in cryptocurrencies or via blockchain (e.g. identification and reporting of activities suspected of money laundering or terrorism financing).

Estate planning and testamentary succession

There are no specific rules as to how cryptocurrencies are treated for purposes of estate planning and testamentary succession. However, cryptocurrencies could be qualified as intangible assets from a Serbian civil law perspective. As such, they do not differ from ordinary assets and can be included in estate planning and testamentary succession.

The newly adopted DAA does not explicitly provide rules regarding estate planning and testamentary succession.

Bojan Rajić
Tel: +381 60 3202 632 / Email: B.Rajic@schoenherr.rs

Bojan Rajić specialises in corporate/M&A and employment. Bojan advises international clients on their market entry and is a member of the team that provides full-service transactional support in the implementation of their investments. He is a specialist of contracts and investments incentives. He advised on the sale of IT start-up 3Lateral to Epic Games, Smurfit Kappa Group on the acquisition of the largest integrated packaging business in Serbia, and Telenor on the sale of its subsidiary in Serbia. He advised Adient Seating on the establishment of a new plant in Serbia, including in relation to relevant subsidies and negotiations of the corresponding grants agreement. Recently, Bojan acted as legal counsel and provided all M&A, regulatory and general corporate services to Solelos (former Gamecredits), an IT company operating various blockchain-based and cryptocurrency projects.

Mina Mihaljčić
Tel: +381 60 3202 620 / Email: M.Mihaljcic@schoenherr.rs

Mina Mihaljčić is an attorney at law and has been with the firm since 2017. She specialises in corporate/M&A. She has advised clients in the IT, telecommunications, banking and finance, and packaging industries. Most recently, she advised on the sale of an innovative technologies developer from Serbia to Epic Games and the leading telecom operator on the acquisition of a major cable television, broadband internet and mobile service provider. Mina acted as legal counsel and provided all M&A, regulatory and general corporate services to Solelos (former Gamecredits), an IT company operating various blockchain-based and cryptocurrency projects.

Moravčević Vojnović i Partneri AOD Beograd
in cooperation with Schoenherr

Bulevar vojvode Bojovića 6–8, 11000 Belgrade, Serbia
Tel: +381 11 3202 600 / URL: www.schoenherr.rs

Singapore

Kenneth Pereire & Lin YingXin
KGP Legal LLC

Government attitude and definition

The Singapore Government takes a pragmatic, practical 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, such as Singapore's "Project Ubin", to explore the use of blockchain and distributed ledger technology for the clearing and settlement of payments and securities.[1] 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. The MAS has also partnered with the Bank for International Settlements Innovation Hub and the community on a new initiative entitled "Project Dunbar", to design, develop and test new multi-central bank digital currency models for cross-border payments involving wholesale central bank digital currencies.[2]

Cryptocurrency regulation

Cryptocurrencies are either regulated or unregulated under Singapore's Payment Services Act 2019 ("**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 (Cap. 289) ("**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".

A "digital payment token exchange" refers to "a place or facility where offers or invitations to buy or sell any digital payment token in exchange for any money or any other digital payment token, are regularly made on a centralised basis, those offers or invitations are intended, or may reasonably be expected, to result (whether directly or indirectly) in the acceptance of those offers or in the making of offers to buy or sell digital payment tokens in exchange for money or other digital payment tokens, as the case may be, and the person making any such offer or invitation, and the person accepting that offer or making an offer in response to that invitation, are different persons". However, it does not include a place or facility (whether electronic or otherwise) that is used exclusively by one person to make offers or invitations to buy or sell any DPT in exchange for any money, or any DPT, and/or to accept any offer to buy or sell any DPT in exchange for any money, or any DPT.

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 the 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 the MAS for the performance of its obligations to its payment service customers, following amendments to the PSA introduced in 2021, the MAS is now empowered 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 as 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 the 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 (Cap. 48A), 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.

The 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.

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 for, 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 for, among other things, the total amount raised from the offers within any period of 12 months to not 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 (Cap. 65A) ("**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 (Cap. 325) ("**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 the MAS could apply to the person. Following the 2021 amendments to the PSA expanding the scope of DPT services to also include facilitating the exchange of DPTs where the service provider or intermediary platform does not even come into possession with the monies or DPTs involved, such virtual asset service providers and crypto intermediaries may also now come under the regulatory ambit of the 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 the 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.

In addition, DPT service providers may be subject to additional requirements that the 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 the MAS. Based on our experience of dealing with the MAS, the additional requirements that the MAS may impose at its discretion include imposing a requirement for the DPT service provider to procure a banker's guarantee, professional indemnity insurance or even to lodge a security deposit with the MAS prior to the MAS issuing the operating licence to the DPT service provider. The 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 Licensee should verify the due authority of each natural person appointed to act on behalf of the customer by obtaining at least the appropriate documentary evidence

authorising the appointment of such natural person by the customer to act on his or its behalf and the specimen signature of such natural person appointed.

The Licensee should identify the beneficial owners, if any, in relation to its customers, and take reasonable measures to verify the identities of the beneficial owners using the relevant information or data obtained from reliable, independent sources.

The Licensee should, when processing the application to establish business relations or to undertake a relevant business transaction without an account being opened, understand and, as appropriate, obtain from the customer information as to the purpose and intended nature of such account relationship or relevant business transaction.

Where the Licensee undertakes one or more relevant business transactions for a customer without an account being opened, the Licensee should review the earlier relevant business transactions undertaken by that customer to ensure that the current relevant business transaction is consistent with the Licensee's knowledge of the customer, its business and risk profile and, where appropriate, the source of funds.

Where the Licensee establishes an account relationship with a customer, the Licensee should review any relevant business transaction undertaken before the business relations are established, to ensure that the business relations are consistent with the Licensee's knowledge of the customer, its business and risk profile and, where appropriate, the source of funds.

Where the Licensee suspects that two or more transactions are or may be related, linked or the result of a deliberate restructuring of an otherwise single transaction into smaller transactions in order to evade the Licensee's customer due diligence measures, the Licensee should treat the transactions as a single transaction and aggregate their values.

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

The 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 the 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.

The MAS has indicated in the Fintech Regulatory Sandbox Guidelines issued in November 2016 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. The 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' moneys 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 the 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 (Cap. 289) 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 (Cap. 110), 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 Bitcoin 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 (Cap. 289) or the Commodity Trading Act (Cap. 48A).

Border restrictions and declaration

There are currently no border restrictions or declarations required with respect to cryptocurrencies.

Reporting requirements

For unregulated entities, they would have to comply with the reporting requirements under the CDSA (Cap. 65A) and the TSFA (Cap. 325).

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 the

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 (Cap. 289) 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 (Cap. 146), the Wills Act (Cap. 352), and the Probate and Administration Act (Cap. 251), 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.

* * *

Endnotes

1. https://www.mas.gov.sg/schemes-and-initiatives/Project-Ubin.
2. https://www.bis.org/about/bisih/topics/cbdc/wcbdc.htm.

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 was admitted as an Advocate and Solicitor of the Supreme Court of Singapore 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 enterprises, and multi-national corporations from various industries, including financial technology, finance, education, bio-technology, 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 all kinds of contracts and documentation. He has experience handling arbitration cases and litigation in the High Court of Singapore.

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

Government attitude and definition

The Spanish government has been very cautious and conservative with regard to cryptocurrencies, since Spanish law is highly protective of the rights of investors and consumers and because, during the recession, there has been a large number of cases of financial and securities fraud. Cryptocurrency cannot be legally treated as money for legal tender. Law 46/1998 of 17 December, on the introduction of the euro as the national currency, provided that from 1 January 1999, the national currency of Spain shall be the euro. This Law cross-refers to Council Regulation (EC) 974/98 of 3 May 1998. Under article 10 of this Regulation, only banknotes and coins denominated in euros and valid in other Eurozone countries shall have the status of legal tender in Spain and, more generally, the euro shall be the sole unit of account in legal instruments, whether under private or public law. We have recently studied a proposal from the Spanish Stock Market Regulator ("CNMV"), which has been granted the power to regulate the aggressive advertisement of cryptocurrencies. The proposal gives us a normative definition of crypto assets, stating that a crypto asset is a "[d]igital representation of an asset or right that can be electronically transferred or stored by using distributing ledger technologies or other similar ones". This Circular will enter into force three months after its publication in the Spanish National Gazette (*Boletín Oficial del Estado*). Regarding blockchain technology, it is fair to say that a technology that allows digital information to be distributed, but not to be copied, will have many uses in the Spanish legal environment. In Spain, notaries have a monopoly on certifying the authenticity of legal documents, so blockchain platforms could be an alternative to notaries for the documentation of certain legal documents. A recent example has been a syndicated financing carried out by a major bank (BBVA) based on a blockchain platform.

Cryptocurrency regulation

There is no specific regulation on cryptocurrencies in Spain, except that they cannot be treated as legal tender, which is exclusively reserved for the euro as the national currency. The abovementioned joint *communiqué* also points out that there are no issues for cryptocurrencies or initial coin offerings ("ICOs") that have been approved or verified by any regulatory authority such as the Bank of Spain or the CNMV. In Spanish law, a cryptocurrency cannot be considered a financial instrument (promissory note, derivative, etc.) either, nor a currency (domestic or foreign), but we consider that they could be assimilated to securities in the case of public offerings, or to chattels or commodities when they are traded individually.

To the extent they can be considered securities, ICOs may fall within the prospectus-filing requirements of the Spanish stock market law ("LMV"), as the definition of financial

instruments and negotiable securities is very wide (article 2 LMV), and the Spanish government can add new types of securities by its own fiat without an amendment of the law being necessary, provided this has been agreed under EU regulations. A *communiqué* of the CNMV dated 8 February 2018 has also confirmed this view and therefore ratified it by a notice, dated 6 July 2018. Under article 38 of Royal Decree 1310/2005, as amended from time to time, offerings addressed exclusively to professional investors or to fewer than 150 persons, or with a minimum investment of at least EUR 100,000 per investor, or in the case of securities having a face value of at least EUR 100,000, would not be subject to the prospectus-filing requirements (CNMV).

As discussed, the Spanish regulator (CNMV) is highly protective of small investors' rights. This may have had an impact on the non-advertisement of ICOs in the Spanish market so far. On the other hand, the CNMV is also sensitive to the benefits of ICOs, to the extent they bring technological innovation and may promote entrepreneurial business. The current position of the CNMV and the Bank of Spain is that specific regulation of cryptocurrency and ICOs is necessary, but such regulation can only be made at EU level and after consultation with certain third countries, such as the U.S., that play a major role in world financial markets (see statement to the press by Sebastián Albella, Chairman of the CNMV, *El Economista*, dated 9 June 2018). In addition, on a European level, the President of the European Central Bank, Christine Lagarde, called for a global regulation on Bitcoin due to it being a "highly speculative" asset, and the European Commission recently published the first proposal in history to regulate Markets in Crypto Assets ("MiCA").

Although there is no specific regulation on cryptocurrencies in Spain, there are a few things that have to be taken into account. First of all, there is a new draft Circular by the CNMV, the objective of which is to develop the norms, principles and criteria to be complied with by cryptocurrency advertisement. The Circular incorporated a few definitions such as "Cryptoassets" and "Cryptoasset Service Providers", as well as defining what will constitute an "Advertising Campaign" and a "Massive Advertising Campaign" in the cryptoworld. The rule establishes that advertisement campaigns targeted towards Spanish residents will only be subject to prior notice to the CNMV when they are Mass Campaigns (directed to more than 100,000 people). All other campaigns will be exempt from this requirement. Nonetheless, the CNMV might oblige certain Cryptoasset Service Providers to always comply with the prior notice if they deem the impact of their campaigns too high for the public.

On a more general note, the Circular states that all advertisement campaigns shall be tied to general principles stated in Annex 1 of the Circular, such as being clear, impartial and not misleading.

The Circular is to enter into force three months after its publication and the period for public consultations to the CNMV ended on 1 September. Nonetheless, interested parties, especially crypto exchanges, still remain with many doubts, soliciting the CNMV to broaden their criteria for what constitutes "clear" and "not misleading" advertisement, as well as to clarify the notification periods and the concept of "Massive Advertising Campaigns".

Sales regulation

To the extent cryptocurrencies are considered commodities, they will be traded under the general rules of the Civil Code and the Code of Commerce, and in particular, those applicable to the contract of barter (permute). We will see in a few months the entry into

force of the European Commission's regulation on markets for crypto assets, which will stir up regulation concerning sales on this sphere. Aside from Spanish law that would allow the parties freedom of choice of the governing law, applicable to the transaction (article 3 of the Rome I Regulation, 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 the Rome I Regulation), 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 via the internet. Thus, much depends on how Spanish law would characterise cryptocurrencies. The Bank of Spain and the CNMV seem to consider them as a "[d]igital representation of an asset or right that can be electronically transferred or stored by using distributing ledger technologies or other similar ones" based on the Circular that the CNMV recently published. 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

Capital gains from the sale of cryptocurrencies by a person resident in Spain will be taxed according to a variable rate from 19–23%. The higher rate applies for gains in excess of EUR 50,000.

On 10 July 2021, the Spanish National Gazette published Law 11/2021 on preventive measures to combat tax avoidance, a long-awaited transposition of EU Council Directive 2016/1164 laying down rules against tax avoidance practices that directly affect the functioning of the internal market.

This new Law brought to light new obligations for cryptocurrency service providers in Spain acting as intermediaries, such as: (i) providing information on balances concerning every different virtual currency and, as the case may be, on fiat currency, as well as the identification of the owners, authorised persons and beneficiaries of such balances; (ii) on acquisitions, transmissions and exchanges related to crypto assets, as well as any payments and collections performed in cryptocurrencies in which they participate (they must submit a list of the parties involved in the transaction, indicating their domicile, tax ID number, class and number of crypto assets, as well as the price and date of the transaction); and (iii) residents, entities, and permanent establishments of residents abroad that make initial offerings of new cryptocurrencies, will have the obligation to report their delivery in exchange of other crypto assets or legal currency.

For these three obligations, there are still certain clarifications to be made, including: (i) exempt thresholds, if any, under which there may be no obligation to file the return; and (ii) the deadline and specific tax form to provide the information to the authorities. All of these parameters, nonetheless, will be determined by the Ministry of Treasury through regulatory dispositions.

Nonetheless, it is likely that the thresholds for reporting cryptocurrencies could be similar to those for bank transfers, which report from EUR 10,000 per transfer and EUR 3,000 for cash deposits.

The Law does not establish specific penalties in the event of a failure to provide this information on time. Therefore, it is foreseen that general sanctions may apply.

On the other hand, the Law also includes declaratory obligations for crypto asset owners. In other words, crypto assets are added within the list of goods that have to be reported in the Informative Declaration on Assets and Rights located abroad (Form 720).

Money transmission laws and anti-money laundering requirements

On 28 April 2021, the Spanish National Gazette published Royal Decree 7/2021 of 27 April, for the transposition of the EU directives on the areas of competition, prevention of money laundering and credit institutions. This Royal Decree will modify Law 10/2010 of 28 April, for the Prevention of Money Laundering and Financing of Terrorism, a topic of concern for all governments in relation to crypto assets being used for unlawful purposes. There are several definitions included in the modified article 1 of Law 10/2010 such as one 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." There were also new regulated entities incorporated in article 2 of Law 10/2010. Among these entities, the "providers of services regarding the exchange between virtual and fiat currency, and the custody of virtual wallets" can be found in section z) of article 2 (hereinafter, "Virtual Currency Service Providers").

The Spanish Central Bank ("SCB") has a period of six months for the registry for these Virtual Currency Service Providers to start functioning counting from the date of entry into force of Royal Decree 7/2021 (29 April 2021).

Promotion and testing

The Spanish government has recently approved Law 7/2020, on the digital transformation of the financial system, which provides for the creation of test space for financial innovations subject to administrative supervision ("Regulatory Sandbox"). It is an attempt to change the 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 appointed to carry out the follow-up, and if testing is satisfactory, licences will be granted. Spanish law seems to be drawing its inspiration from the UK's Financial Conduct Authority, which grants licences for sandboxes. The idea 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 the 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: The 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 several decentralised finance and blockchain projects currently in sandboxes as well as many other areas.

Ownership and licensing requirements

Virtual Currency Service Providers will now have to comply with the following provisions:

1. Regardless of their nationality, if 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 within the Registry of the SCB created for these purposes.
2. Likewise, the following must also register within 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. The entities located in Spain that provide these services, regardless of the location of the service recipients.
3. Registration within the SCB Registry will be conditioned to the existence of:
   a. Adequate anti money-laundering prevention procedures, provided by Law 10/2010 (identification of clients, communications to SEPBLAC (Spain's Financial Intelligence Unit), internal control measures, etc.).
   b. Compliance with the requirements of commercial and professional honourability, according to the terms established in article 30 of Royal Decree 84/2015 of 13 February, for the development of Law 10/2014 of 26 June, on the regulation, supervision and solvency of credit institutions. In summary, these requirements consist of displaying personal, business and professional conducts that do not cast doubt on the ability to perform sound and prudent management of the entity.
   c. The SCB will have authority to supervise the compliance of the aforementioned requirements.

It is important to highlight that if Virtual Currency Service Providers do not comply with the required registration mentioned 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. The infringement will be considered "serious" and not "very serious" only if the provided services were occasional or isolated.

Mining

Bitcoin and many other cryptocurrencies are not yet regulated, and this is permitted except as discussed in "Cryptocurrency regulation", above.

Border restrictions and declaration

As mentioned before, the new Law 11/2021 on preventive measures to combat tax avoidance has included virtual currency (such as crypto assets) in the list of goods that have to be reported in the Informative Declaration on Assets and Rights located abroad (Form 720).

This obligation is applicable to owners, beneficiaries, authorised persons or any individual or entity with power of disposition over such assets.

The thresholds to report on crypto assets located abroad could also be similar to those established by the tax authorities for other goods and rights located abroad, such as real estate acquired for more than EUR 50,000, bank accounts with more than EUR 50,000 (average amount in the fourth quarter of the year), and shares, bonds, annuities or insurances of more than EUR 50,000 per year.

Reporting requirements

Systematic reporting requirements

Article 27 of the Regulation of Law 10/2010 of 28 April, approved by Royal Decree 304/2014 of 5 May, states that obliged subjects (among which cryptocurrency service providers are now included) shall report to the Spanish anti-money laundering authorities (SEPBLAC) on a monthly basis in accordance with the following conditions:

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 13 November, on payment services, shall report to SEPBLAC those 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 who are resident, or those acting on their behalf, 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 of 28 April, which would be: (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 of 28 April, on the prevention of money laundering and terrorist financing, 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 payment:

- 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.

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 López-Ibor Aliño is the managing partner of the Madrid office. Previously, he was managing partner of Allen & Overy, Madrid, for 10 years. He specialises in commercial, financial and banking law. Alfonso is also recognised for his experience in litigation, arbitration and air transport law.

In commercial law, he regularly advises clients on the acquisition and sale of Spanish and foreign companies, in venture capital/private equity transactions, MBOs and corporate restructuring. He also advises multinationals that wish to settle in Spain, either through branches or through the acquisition of already established companies.

In banking and financial law, he has experience in syndicated loans, guarantees and financing of assets, as well as with working with the CNMV.

Alfonso heads up the department specialised in providing legal advice to companies in the airline sector, including national and international contracting, handling contracts, financial structures, including operating lease transactions, guarantees, financing of acquisitions, permits, authorisations and registrations. He is one of the best-known Spanish lawyers in the aviation sector.

Alfonso provides advice on litigation and international arbitrations in matters of great complexity.

Olivia López-Ibor Jaume
Tel: +34 915 21 78 18 / Email: olivia.lopezibor@l-ia.com

Olivia López-Ibor Jaume is a lawyer in the Banking & Finance Department in Madrid. She began her professional career in the Financial Law Department at Allen & Overy.

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.

She advises foreign companies in various securities market operations, including negotiations of guarantee and financing of acquisitions packages and CNMV authorisations. Olivia also advises companies engaged in technology in the e-banking sector, payment services, cryptocurrencies, and on Fintech sector regulation in general.

López-Ibor Abogados

López de Hoyos 35, 3 piso, 28002, Madrid, Spain
Tel: +34 915 21 78 18 / URL: www.lopez-iborabogados.com

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**"), which came into force on August 1, 2021 under the DLT-Law, 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, these tokens are "purely factual intangible assets".[6] Examples of such 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 points out 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.[9] However, other types of stablecoins use stabilisation mechanisms without a direct linkage to any underlying or collateral, as the case may be. Although a number of 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.[10]

Cryptocurrencies are not legal tender

In Switzerland, cryptocurrencies do not qualify as legal tender.[11] 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.[12] 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.[13]

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)[14] and successfully demonstrated the feasibility of settling tokenised assets with wholesale central bank digital currencies ("**wholesale CBDC**").[15] On June 10, 2021, the SNB, together with the Banque de France and the BIS Innovation Hub, also announced an experiment in the use of digital central bank money for financial intermediaries (wholesale CBDC) to settle cross-border transactions.[16] Nevertheless, it cannot yet be concluded that the SNB will issue such a digital currency.

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.[17]

Introduction of DLT-Securities

The DLT-Law has 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.[18] 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.[19] 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.[20] 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.[21]

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.

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.

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*).[22] 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 at the point of issue. This view on payment and utility tokens is supported by the Dispatch.[23]

Currently,[24] FINMA has the following view on whether tokens qualify as securities:[25]

- 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**"),[26] which entered into force on January 1, 2020, remains unclear. 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 met, the typical "connection with capital markets" inherent to securities, according to FINMA, does not exist. FINMA points out 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.[27] Also, in the case of a linkage 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.[28] Generally, if and to the extent that stablecoins are structured as tokens, whose values are derived from one or more underlying asset(s) and that they 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 represent derivatives within the meaning of FinSA and FMIA (defined above). Since, under Swiss law, securities 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.[29] 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.[30] 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.[31]

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**");[32]

(ii) Swiss trading platform regulations under the FMIA;[33] and/or (iii) Swiss prospectus requirements and further regulations in connection with financial services under FinSA.

- Persons creating certain types of securities tokens and/or trading in securities tokens 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 may trigger various regulations under FinSA provided that, among other things, the securities firm is qualified as a "financial service provider" and the securities tokens qualify as "financial instruments" within the meaning of FinSA. 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 an issuing 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 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.[34] 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, which also came into effect on August 1, 2021, 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 at a DLT-Trading Venue. The DLT trading facilities 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

FINMA recently issued two approvals to financial market infrastructures that operate based on DLT. SIX Digital Exchange AG has been authorised by FINMA to act as a central securities depository and the associated company SDX Trading AG (collectively, "**SDX**") to act as a stock exchange.

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.[35] 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.

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 a 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.[36]

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**").[37]

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).[38]
- *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.[39] This legislative initiative has been implemented and consists of three pillars:

- The first pillar, in force since August 1, 2017, the Swiss "sandbox" exemption, allows companies to engage in activities that would usually trigger bank licensing requirements. According to the Swiss Banking Act,[40] 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.[41] 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, in force since August 1, 2017, 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 foreign exchange 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 foreign exchange traders is currently not clear.
- The third pillar, in force since January 1, 2019, 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 may be legally owned. With regard to tokens that do not qualify as securities, *i.e.*, cryptocurrencies such as Bitcoin, the ownership question is

currently 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.[42]

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 service, is required to obtain a FinTech licence (see above, "Promotion and testing"), whereby such crypto-based assets may not be invested nor interest-bearing.[43] 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.[44]

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".[45] 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.[46] 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.[47] 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.[48] Likewise, stablecoins that are linked to individual properties or a portfolio of properties may, according to FINMA, represent collective investment schemes.[49]

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 cryptocurrencies 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.[50] Further, mining of cryptocurrencies does not generally qualify as a financial service within the meaning of FinSA.[51]

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.

Cryptocurrencies such as Bitcoin are considered to have an inheritable value.[52] 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. *Cf.* https://stablecoinindex.com/.
10. *Cf.* https://blockchain.capital/the-business-of-stablecoins/; https://blockchainwelt.de/stablecoins-sind-preisstabile-kryptowaehrungen-moeglich/.
11. 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.
12. *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.
13. https://www.snb.ch/en/mmr/speeches/id/ref_20190905_tjn/source/ref_20190905_tjn.en.pdf.
14. *Cf.* https://www.snb.ch/de/mmr/reference/pre_20191008/source/pre_20191008.de.pdf.
15. *Cf.* https://www.bis.org/publ/othp35.pdf; https://www.snb.ch/en/mmr/reference/pre_20201203/source/pre_20201203.en.pdf.

16. https://www.snb.ch/en/mmr/reference/pre_20210610/source/pre_20210610.en.pdf.
17. *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.
18. 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).
19. *Cf.* Kramer/Oser/Meier, *Tokenisierung von Finanzinstrumenten de lege ferenda*, in: Jusletter May 6, 2019, N 22; Dispatch, p. 107 *et seq*.
20. *Cf*. Dispatch, p. 277.
21. *Cf*. Federal Council Explanatory Report – DLT-Draft Law, p. 29; Dispatch, p. 277.
22. According to the DLT-Draft Law, DLT-Securities may also classify as securities; *cf.* Dispatch, p. 309.
23. *Cf.* Dispatch, p. 309.
24. 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.
25. *Cf.* FINMA ICO Guidelines, p. 4 *et seq*.
26. Federal Act on Financial Services of June 15, 2018, SR 950.1.
27. FINMA Supplement, p. 3.
28. FINMA Supplement, p. 4.
29. *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.
30. https://www.finma.ch/en/news/2021/09/20210929-mm-genehmigung-schweizer-kryptofonds/.
31 https://www.cryptofinance.ch/wp-content/uploads/2021/09/20210929_Crypto-Finance_Press_Release_Launch_Swiss_fund_EN.pdf.
32. Federal Act on Financial Institutions of June 15, 2018, SR 954.1.
33. Federal Act on Financial Market Infrastructures and Market Conduct in Securities and Derivatives Trading of June 19, 2015, SR 958.1.
34. Federal Council Report – Legal framework for distributed ledger technology and blockchain, p. 122; Dispatch p. 309 *et seq*.
35. *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.
36. *Cf*. Swiss Legal Tech Association (SLTA), Regulatory Task Force Report, p. 34.
37. Federal Act on Anti-Money Laundering of October 10, 1997, SR 955.0.
38. *Cf.* FINMA ICO Guidelines, p. 6; FINMA Supplement, pp 2 and 7.
39. https://www.admin.ch/gov/en/start/documentation/media-releases.msg-id-64356.html.
40. Federal Act on Banks of November 8, 1934, SR 952.0.
41. *Cf.* Arts 2 and 6 of the Swiss Banking Ordinance of April 30, 2014, SR 952.02.
42. *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.

43. *Cf*. Art. 1b of the Banking Act.
44. *Cf*. Art. 4*sexies* of the Banking Act.
45. *Cf.* FINMA Supplement, p. 2.
46. *Cf*. FINMA Supplement, p. 2 *et seq*.
47. *Cf.* FINMA Supplement, p. 2 *et seq.*
48. *Cf.* FINMA Supplement, pp 2–4.
49. *Cf.* FINMA Supplement, p. 4.
50. See also, Federal Council Report – Legal framework for distributed ledger technology and blockchain, p. 139.
51. Federal Council Report – Legal framework for distributed ledger technology and blockchain, p. 117.
52. *Cf*. Eigenmann/Fanti, *Successions, Données Personnelles, Numériques et Renseignements*, in: SJ 2017 II, p. 198.

* * *

Acknowledgment

The authors acknowledge with thanks the contributions of Armin Mandzuka 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, financial services regulation as well as corporate and commercial law. 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 currencies.

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). The FSC further issued a press release on 19 December 2017 ("2017 Release"), 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 of 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 – 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$100 million. A platform can accept to process a second STO only one year 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 as 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, currently there 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 the 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 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 no-name basis both for the transferor and transferee – the effective date of such provision will be further determined and announced by the FSC.

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 would 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, nine applications have been approved by the FSC to enter into the sandbox, but 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 the 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 the 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 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

United Kingdom

Stuart Davis, Sam Maxson & Andrew Moyle
Latham & Watkins

Government attitude and definition

UK policy thinking in relation to cryptocurrencies is still actively developing. It was first set out by the UK Cryptoassets Taskforce in its Final Report[1] (the "**Taskforce Report**"), published in October 2018, and has subsequently been developed through further work by the Taskforce authorities (HM Treasury, the Bank of England and the UK Financial Conduct Authority ("**FCA**")).

The Taskforce Report identified cryptocurrencies as a subset of the broader category "cryptoasset". It defined the latter as "a cryptographically secured digital representation of value or contractual rights that uses some type of [distributed ledger technology ("**DLT**")] and can be transferred, stored or traded electronically".[2] Within this overarching category, the Taskforce Report identified three sub-categories and offered the following (non-legislative) definitions:

"A. **Exchange tokens** — which are often referred to as 'cryptocurrencies' such as Bitcoin, Litecoin and equivalents. They utilise a DLT platform and are not issued or backed by a central bank or other central body. They do not provide the types of rights or access provided by security or utility tokens, but are used as a means of exchange or for investment.

B. **Security tokens** — which amount to a 'specified investment' as set out in the Financial Services and Markets Act (2000) (Regulated Activities) Order […]. 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 […].

C. **Utility tokens** — which can be redeemed for access to a specific product or service that is typically provided using a DLT platform."[3]

Although UK financial regulators have issued warnings in relation to investment in cryptoassets,[4] they are not subject to a blanket prohibition or ban in the UK. However, as indicated by the definitions set out in the Taskforce Report, some cryptoassets will be subject to financial regulation (see *Cryptocurrency regulation* below). UK payment services and electronic money regulation may also be relevant, and the UK anti-money laundering ("**AML**") regime has been extended to capture activities relating to most cryptoassets (including cryptocurrencies), regardless of whether they are otherwise subject to financial regulation (see *Money transmission laws and anti-money laundering requirements* below). Cryptoassets (including cryptocurrencies) are not considered money or equivalent to fiat currency in the UK.

As noted above, the Taskforce authorities have continued to conduct further substantive work in relation to cryptoassets since the publication of the Taskforce Report. In particular:

- The FCA consulted on[5] and published[6] regulatory guidance in relation to cryptoassets (including cryptocurrencies) (the "**FCA Guidance**"). It also consulted on[7] and introduced[8] from 6 January 2021 a ban on the sale, marketing and distribution of derivatives and exchange-traded notes referencing "unregulated transferable cryptoassets" in or from the UK to retail customers.
- At the time of writing, responses are expected to two consultations on cryptoassets by HM Treasury: the first relating to changes to the UK financial promotions regime with a view to bringing otherwise unregulated cryptoassets (including cryptocurrencies) into scope (see *Sales regulation* below); and the second relating to the UK regulatory approach to cryptoassets more generally, with a focus on stablecoins (see *Cryptocurrency regulation* below).
- Although it has not decided on whether to introduce a central bank digital currency ("**CBDC**"),[9] the Bank of England has published a discussion paper on what such a CBDC would look like and has jointly created a Central Bank Digital Currency Taskforce with HM Treasury to coordinate the exploration of a potential UK CBDC.[10]

Cryptocurrency regulation

As noted above, there is no blanket prohibition or ban on cryptocurrencies in the UK. Nor does the UK have a bespoke financial regulatory regime for cryptoassets (notwithstanding that certain elements of the UK AML regime apply specifically in relation to cryptoasset business). Accordingly, whether or not a given cryptocurrency is subject to financial regulation in the UK depends on whether it falls within the general financial regulatory perimeter established under the Financial Services and Markets Act 2000 ("**FSMA**") or, as discussed in *Money transmission laws and anti-money laundering requirements* below, within the UK AML regime or the payment services and electronic money regime established under the Payment Services Regulations 2017 ("**PSRs**") and the Electronic Money Regulations 2011 ("**EMRs**").

This is reflected in the cryptoasset "taxonomy" set out in the FCA Guidance, which broadly follows the definitions set out in the Taskforce Report, but which has been refined by the FCA as follows:

Taskforce Report taxonomy	FCA Guidance taxonomy[11]
Security tokens — which amount to a 'specified investment' as set out in the Financial Services and Markets Act (2000) (Regulated Activities) Order […]. 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 […].	**Security tokens**: These are tokens that amount to a 'specified investment' under the Regulated Activities Order (RAO), excluding e-money. 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 other financial instrument under the EU's Markets in Financial Instruments Directive II (MiFID II). These tokens are likely to be inside the FCA's regulatory perimeter.
	E-money tokens: These are tokens that meet the definition of e-money under the Electronic Money Regulations (EMRs). These tokens fall within regulation.

Taskforce Report taxonomy	FCA Guidance taxonomy[11]
Exchange tokens — which are often referred to as 'cryptocurrencies' such as Bitcoin, Litecoin and equivalents. They utilise a DLT platform and are not issued or backed by a central bank or other central body. They do not provide the types of rights or access provided by security or utility tokens, but are used as a means of exchange or for investment.	**Unregulated tokens**: Any tokens that are not security tokens or e-money tokens are unregulated tokens. This category includes utility tokens which can be redeemed for access to a specific product or service that is typically provided using a DLT platform. The category also includes tokens such as Bitcoin, Litecoin and equivalents, and often referred to as 'cryptocurrencies', 'cryptocoins' or 'payment tokens'. These tokens are usually decentralised and designed to be used primarily as a medium of exchange. We sometimes refer to them as exchange tokens and they do not provide the types of rights or access provided by security or utility tokens, but are used as a means of exchange or for investment.

In summary, the FCA Guidance taxonomy splits cryptoassets into regulated and unregulated cryptoassets. The Taskforce Report definitions of exchange tokens and utility tokens are retained, and these two sub-categories of cryptoassets comprise "unregulated tokens" in the FCA Guidance taxonomy. Cryptoassets that constitute electronic money are split out from the Taskforce Report sub-category of security tokens, and are instead labelled as "e-money tokens", and these two sub-categories of cryptoassets (i.e., security tokens other than e-money tokens and e-money tokens) comprise "regulated tokens" in the FCA Guidance taxonomy.

The kinds of instruments that are regulated under FSMA are set out in an exhaustive fashion in the Financial Services and Markets Act 2000 (Regulated Activities) Order 2001 ("**RAO**"). These are known as "specified investments" and include instruments such as shares, bonds, fund interests and derivative contracts. Therefore, in order to determine whether a given cryptocurrency is subject to financial regulation in the UK, it is necessary to analyse whether it matches the definition of a specified investment in the RAO. Those cryptoassets that do are labelled "security tokens" in the FCA Guidance and will typically be subject to UK financial regulation.

As stated by the FCA: "Any tokens that are not security tokens or e-money tokens [as to which see *Money transmission laws and anti-money laundering requirements* below] are unregulated tokens."[12] In practice, this analysis proceeds predominantly on the basis of an "intrinsic" assessment of a given cryptocurrency, focused on the rights or entitlements granted to holders, rather than being based on "extrinsic" factors, such as the intended or actual use of the relevant cryptocurrency or other contextual factors relating to the cryptoasset (such as whether a platform to which the cryptoasset relates is currently operational or whether the network underlying the cryptoasset is decentralised).[13]

Although characterisation of cryptocurrencies in this way must be undertaken on a case-by-case basis in order to determine definitively whether they are subject to UK financial regulation, the FCA Guidance provides useful indicators of the likely outcome of any such analysis. "Classic" cryptocurrencies (such as Bitcoin, Litecoin and Ether), which are not centrally issued and give no rights or entitlements to holders, are labelled "exchange tokens" in the Taskforce Report and "unregulated tokens" in the FCA Guidance. As explained in the FCA Guidance, exchange tokens "typically do not grant the holder any of the rights associated with specified investments".[14] Accordingly, in the FCA's view:

> "Exchange tokens currently fall outside the regulatory perimeter. This means that the transferring, buying and selling of these tokens, including the commercial operation of cryptoasset exchanges for exchange tokens, are activities not currently regulated by the FCA.

> For example, if you are an exchange, and all you do is facilitate transactions of Bitcoins, Ether, Litecoin or other exchange tokens between participants, you are not carrying on a regulated activity."[15]

It is therefore clear that activities related to Bitcoin, Litecoin and Ether are currently unlikely to trigger licensing requirements in the UK (although registration under the recently extended UK AML regime may be required). Cryptocurrencies with substantially similar features (i.e., those that are not centrally issued and do not grant any rights or entitlements to holders) are also currently unlikely to trigger licensing requirements in the UK (although, again, registration under the UK AML regime may be required). The same is also true for utility tokens. The fact that these kinds of cryptoassets may be used for speculative investment purposes in addition to being used as a means of exchange or to redeem a service should not impact this conclusion.

Stablecoins are an increasingly popular type of cryptoasset that are typically more difficult to characterise for financial regulatory purposes than classic cryptocurrencies. Broadly, a stablecoin is a cryptoasset that by design seeks to maintain a stable market value, typically through pegging the value of the stablecoin to underlying assets or currencies (such as gold or USD). Often, stablecoins are primarily intended to be utilised as a means of exchange much like classic cryptocurrencies. Pegging the value of a stablecoin to an underlying asset or currency can be achieved in a variety of ways, and the precise structure adopted by a given stablecoin will determine whether it is classified as a specified investment in the UK. For example, a "fully collateralised" stablecoin issued by a central issuer that is pegged to an underlying reference asset through the issuer holding the relevant underlying reference asset is likely to constitute a specified investment (or, indeed, electronic money) if holders of the stablecoin have rights or entitlements in relation to the underlying reference asset. On the other hand, so-called "algorithmic" stablecoins, which seek to maintain a stable value through the use of algorithms to control supply without any backing by a reference asset, may be unregulated tokens.

HM Treasury is currently consulting[16] on potential changes to the UK financial regulatory framework to establish "a sound regulatory environment" for stablecoins. The potential changes proposed in the consultation constitute part of the UK government's "staged and proportionate approach" to cryptoasset regulation in the UK and HM Treasury notes that "[f]uture regulation of a potentially wider set of tokens and services" will be informed by the government's continuing strategic assessment of new and emerging risks in cryptoasset markets. For now, however, the potential changes are focused on seeking to ensure that cryptoassets that could be reliably used for retail or wholesale transactions are subject to minimum requirements and protections as part of a UK authorisation regime. The consultation is limited to defining the scope of the regulatory perimeter with respect to such stablecoins and establishing the high-level objectives and principles that should frame the detailed requirements that would be applicable to persons falling within the scope of the new authorisation requirement (the consultation states that the UK's financial services regulators will consult on detailed firm requirements should the government adopt the approach set out in the consultation). In-scope cryptoassets for the purposes of the new authorisation requirement would only include those stablecoins that rely on a link to underlying currencies or assets in order to stabilise their value. Exchange tokens, utility tokens and algorithmic stablecoins are therefore likely to remain outside the authorisation perimeter for the time being (but may nevertheless be subject to other aspects of UK financial regulation such as AML regulation or, if extended, financial promotions requirements – see *Money transmission laws and anti-money laundering requirements* and *Sales regulation*

below). Interestingly, the consultation suggests that the definition of in-scope cryptoassets for these purposes may not specify that DLT and cryptography are necessary features, which would be a significant departure from the definition of cryptoasset set out in the Taskforce Report and in UK AML regulation (see *Money transmission laws and anti-money laundering requirements* below). This may also give rise to potential overlap with the existing UK regulatory framework governing payments and electronic money under the PSRs and EMRs (and although this possibility is partially acknowledged in the consultation, it does not include any firm proposals on how this will be addressed). The activities relating to in-scope cryptoassets that the consultation envisages being subject to the new authorisation regime are: issuing, creating or destroying in-scope tokens; value stabilisation and reserve management (including providing custody services in relation to reserve assets); validation of transactions (which could include, for example, the activities of nodes or miners); providing services or support to facilitate access by participants to the network or underlying infrastructure; transmission of in-scope tokens; providing custody and administration of in-scope tokens for third parties; executing transactions in in-scope tokens; and exchanging in-scope tokens for fiat currency. Finally, the consultation also notes that the government is considering the possibility of expressly applying UK payment systems regulation to stablecoin networks that reach a systemically important scale. The potential changes included in the consultation therefore represent significant proposals to clarify and expand the application of the general UK financial regulatory perimeter to certain kinds of stablecoins.

Notably, even if a given cryptocurrency is not a specified investment other than electronic money (i.e., not a security token following the FCA Guidance), certain activities in relation to such cryptocurrencies can currently still be subject to UK financial regulation, and cryptoassets that constitute electronic money (i.e., e-money tokens following the FCA Guidance) are subject to regulation. For example, offering to enter into derivative contracts that reference unregulated cryptocurrencies as their underlying (such as cryptocurrency contracts for differences or Bitcoin futures) by way of business is likely to constitute a regulated activity in the UK for which a person would require authorisation from the FCA. Indeed, such derivatives are also the subject of the FCA ban on their sale, marketing and distribution to retail customers. Establishing, operating, marketing or managing a fund that offers exposure to unregulated cryptocurrencies by way of business may also be subject to UK financial regulation. Furthermore, money transmission laws and AML legislation may also apply to activities carried out in relation to unregulated cryptocurrencies (see *Money transmission laws and anti-money laundering requirements* below).

Sales regulation

The principal sales regulation that is potentially applicable to sales of cryptocurrencies in the UK falls into three broad categories: (i) UK prospectus requirements; (ii) the UK restriction on financial promotions; and (iii) consumer protection and online/distance selling legislation.

UK prospectus requirements

FSMA, in conjunction with the "onshored" UK version of the Prospectus Regulation, imposes requirements for an approved prospectus to have been made available to the public before: (a) transferable securities are offered to the public in the UK; or (b) a request is made for transferable securities to be admitted to a regulated market situated or operating in the UK.[17] Unless an exemption applies (public offers made to qualified investors or fewer

than 150 persons in the UK are, for example, exempt), a detailed prospectus containing prescribed content must be drawn up, approved by the FCA and published before the relevant offer or request is made.

However, these requirements only apply to offers or requests relating to transferable securities. Transferable securities for these purposes are anything that falls within the definition of transferable securities in the "onshored" UK version of the Markets in Financial Instruments Regulation, which captures, for example, shares, bonds and depository receipts (and instruments that give their holders similar rights or entitlements).

Therefore, in order to determine whether these requirements apply to the sale of a given cryptocurrency in the UK, it is necessary to determine whether the cryptocurrency is a transferable security. Referring back to the FCA Guidance, only cryptocurrencies that are security tokens (i.e., only those cryptocurrencies that amount to a specified investment under the RAO other than electronic money) may be transferable securities.[18] Classic cryptocurrencies (such as Bitcoin, Litecoin and Ether) and cryptocurrencies with substantially similar features to classic cryptocurrencies are likely to be regarded as exchange tokens, rather than security tokens. Accordingly, the UK prospectus requirements should not apply to the sales of such cryptocurrencies. Similarly, utility tokens should not amount to transferable securities.

UK restriction on financial promotions

FSMA contains a restriction on financial promotions that applies independently of the UK prospectus requirements. In summary, a person who is not appropriately authorised must not, in the course of business, communicate an invitation or inducement to engage in investment activity in a way that is capable of having an effect in the UK unless the communication is approved by an appropriately authorised person or an exemption applies. Following a consultation in July 2020,[19] HM Treasury has indicated that the government proposes to amend FSMA "when parliamentary time allows" so that in the future, unauthorised persons will only be able to communicate financial promotions that have been approved by an authorised person that has obtained consent from the FCA to provide such approval. Notably, however, the government does not intend this to apply to authorised persons approving the financial promotions of an unauthorised person within the same group, or to the approval of authorised persons' own promotions for communication by unauthorised persons.

For these purposes, the concept of engaging in investment activity is further defined by reference to "controlled activities" and "controlled investments", which are set out in exhaustive fashion in the Financial Services and Markets Act 2000 (Financial Promotion) Order 2005 ("**FPO**"). Therefore, in order to determine whether the restriction on financial promotions applies to particular activities relating to a given cryptocurrency (including, for example, the sale of that cryptocurrency), it is necessary to determine whether the activities involve a controlled activity or a controlled investment by reference to the definitions of each that are set out in the FPO. Although distinct and subtly different, the controlled activities and controlled investments set out in the FPO closely resemble the list of specified activities and specified investments set out in the RAO (discussed in *Cryptocurrency regulation* above).

Typically, therefore, sales of classic cryptocurrencies (such as Bitcoin, Litecoin and Ether) and cryptocurrencies with substantially similar features to classic cryptocurrencies should not currently engage the UK restriction on financial promotions, although analysis of the sale in question must be undertaken on a case-by-case basis in order to determine definitively that this is the case (and related offerings, such as funds providing exposure to unregulated

cryptocurrencies, may well trigger the restriction). The same is also currently true for utility tokens (which, for the time being, are unlikely to constitute controlled investments) and e-money tokens (since electronic money is notably not a controlled investment, and so promotions in relation to electronic money are generally not within the restriction on financial promotions).

However, by way of a consultation in July 2020,[20] HM Treasury proposed to widen the regulatory perimeter by adding otherwise unregulated cryptoassets to the list of controlled investments and increasing the list of controlled activities to include activities relating to the buying, selling, subscribing for or underwriting of such cryptoassets. Although a response to this consultation from HM Treasury is still awaited at the time of writing, if these proposals are adopted, then marketing in relation to certain activities relating to otherwise unregulated cryptocurrencies would only be permissible if conducted by an authorised firm, if approved by an appropriately authorised person or if an exemption applies. With respect to the latter option, a number of potentially helpful exemptions exist, of which the most likely to be relevant are those relating to financial promotions given to investment professionals, sophisticated investors and high-net-worth individuals/entities.

General advertising, online/distance selling and consumer protection legislation

In addition to sales regulation that arises out of the UK financial regulatory framework, there is a raft of general advertising, online/distance selling and consumer protection legislation that is potentially applicable to sales of cryptocurrencies or the offering of services related to cryptocurrencies (such as exchange or wallet services) in or from the UK.

Some of this legislation, like the Consumer Rights Act 2015 or the Consumer Protection from Unfair Trading Regulations 2008, only applies in relation to consumers (typically defined as individuals acting outside of their trade, business, craft or profession), but where it does, provides consumers with significant statutory rights and remedies against supplies of goods, services and digital content and imposes restrictions on the kinds of contractual terms that can be enforced against consumers. Other legislation, like the Electronic Commerce (EC Directive) Regulations 2002, is of more general application and imposes requirements on businesses that offer or provide goods or services digitally. The application of such legislation may also depend on whether or not the business being conducted is subject to UK financial regulation.

Taxation

Currently, there are no bespoke UK tax rules applicable to cryptoassets (including cryptocurrencies). Therefore, existing tax principles and rules apply generally (although some uncertainty remains as to their application).

The UK tax authority HM Revenue and Customs ("**HMRC**") considers that cryptoassets are cryptographically secured digital representations of value or contractual rights that can be transferred, stored and traded electronically (i.e., the definition adopted by the Taskforce). HMRC has identified four types of cryptoassets: exchange tokens; utility tokens; security tokens; and stablecoins. However, HMRC will look at the facts of each case and apply the relevant tax provisions according to what has actually taken place. 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.

Although there is no definitive policy for the taxation of cryptoassets (including cryptocurrency) in the UK, HMRC has published two policy papers, one relating to the taxation of cryptoassets for individuals, published in December 2018 (and updated in December 2019), and the other relating to the taxation of cryptoassets for businesses,

published in December 2019 (notably, the position in these papers may not be binding on HMRC). The positions set out in the policy papers, and HMRC's guidance in general in relation to the taxation of cryptoassets, are contained in HMRC's Cryptoassets Manual, which at the time of writing was last updated on 8 April 2021.

In the Cryptoassets Manual, HMRC states that the tax treatment of cryptoassets continues to develop due to the evolving nature of the underlying technology and the areas in which cryptoassets are used. As such, HMRC stresses that the facts of each case need to be established before applying the relevant tax provisions according to what has actually taken place (rather than by reference to terminology).

The policy papers and Cryptoassets Manual focus on the taxation of exchange tokens. For security tokens and utility tokens, the guidance may provide the starting principles, but different tax treatments may need to be adopted and further HMRC guidance may be published in due course.

Taxation of individuals

Cryptoassets: tax for individuals[21] sets out HMRC's views about how individuals who hold exchange tokens are to be taxed. This policy paper includes the following helpful general points:

- Capital gains tax ("**CGT**") and income tax ("**IT**") may apply to dealings in cryptocurrencies depending on the circumstances. HMRC has clarified that it does not regard cryptocurrencies as currency or money, and that it does not consider buying and selling cryptocurrencies to be the same as gambling (which largely rules out arguments that cryptocurrencies could be exempt from taxation). Cryptoassets are likely to be property for the purposes of inheritance tax.
- In most cases, HMRC expects that buying and selling of cryptocurrencies by an individual will amount to personal investment activity, meaning that individuals will typically have to pay CGT on any gains they realise upon disposal of the cryptocurrencies (which includes not only selling them for fiat currency but also using them to pay for goods and services, giving them away to another person and exchanging them for another kind of cryptoasset).
- If an individual is engaged in a trade of dealing in cryptocurrencies (an exceptional case, in HMRC's view, and one to be determined in accordance with the existing approach taken towards determining whether an individual is engaged in trading securities and other financial instruments for tax purposes), IT would take priority over CGT, being applied to the individual's trading profits.
- Individuals will be liable to pay IT and National Insurance contributions on cryptocurrencies that they receive as a form of payment from their employer. If the cryptocurrencies are considered readily convertible assets ("**RCAs**"), the IT liability will need to be accounted through Pay-As-You-Earn ("**PAYE**"), and employer National Insurance contributions will also be due. Cryptocurrencies that are not RCAs are still subject to IT and National Insurance contributions, but employers do not have to operate PAYE. The individual must declare and pay HMRC the IT due on any amount of employment income received in the form of cryptoassets. The employer should treat the payment of cryptoassets, which are not RCAs, as payments in kind for National Insurance contributions purposes, and pay any Class 1A National Insurance contributions to HMRC. Broadly, a cryptocurrency will be an RCA if trading arrangements exist, or if such arrangements are likely to come into existence.
- A charge to CGT may also arise if an individual subsequently disposes of cryptocurrencies received from their employer, or tokens received as a result of mining activity or airdrops (regardless of whether or not IT was payable on their receipt).

- A person who is not trading and receives tokens from mining must complete a self-assessment tax return (in pound sterling), treating those tokens as "other taxable income", unless they have received cryptoassets worth less than GBP 1,000 or other untaxed income of less than GBP 2,500.
- If a person is resident but not domiciled in the UK and claims the remittance basis of taxation, income and gains that have a source outside the UK are usually only taxed if they are remitted to the UK. HMRC has taken the view that throughout the time an individual is a UK resident, the exchange tokens they hold as beneficial owner will be located in the UK. As a result, UK resident individuals (whether UK or non-UK domiciled) will be subject to UK tax if they carry out a transaction with their tokens that is subject to UK tax.
- Notably, some cryptoasset exchanges may only keep records of transactions for a short period, or the exchange may no longer be in existence when an individual completes a tax return. The onus is therefore on the individual to keep separate records for each cryptoasset transaction, and these must include:
  1. the type of cryptoasset;
  2. the date of the transaction;
  3. whether the cryptoasset was bought or sold;
  4. the number of units;
  5. the value of the transaction in pound sterling (as at the date of the transaction);
  6. the cumulative total of the investment units held; and
  7. bank statements and wallet addresses, if needed for an enquiry or review.

Taxation of businesses

Cryptoassets: tax for businesses[22] sets out HMRC's views about how transactions involving cryptoasset exchange tokens that are undertaken by companies and other businesses (including sole traders and partnerships) are to be taxed. This policy paper includes the following helpful general points:

- As HMRC does not consider any of the current types of cryptoassets to be money or currency, any corporation tax ("**CT**") legislation that relates solely to money or currency does not apply to exchange tokens or other types of cryptoassets (e.g., the foreign currency rules, the Disregard Regulations relating to exchange gains and losses, and designated currency elections).
- Where the buying and selling, or mining, of exchange tokens amounts to a trade, the receipts and expenses of the trade will form part of the calculation of the trading profit of that business for CT purposes. For example, if a company carrying on a trade accepts exchange tokens as payment from customers, or uses them to make payments to suppliers, the token given or received will need to be accounted for within the taxable trading profits. Similarly, in respect of mining, if a business purchases a bank of dedicated computers to mine exchange tokens, as opposed to mining that uses excess home computer capacity, the mined cryptoassets will probably amount to trade receipts and be taxed in accordance with CT principles.
- If the activity concerning the exchange token is not a trading activity, and is not charged to CT in another way (such as the non-trading loan relationship or intangible fixed asset rules, both discussed below), then the activity may be the disposal of a capital asset. Any gain that arises from the disposal would typically be charged to CT as a chargeable gain. A disposal for these purposes includes not only selling tokens for fiat currency, but also using tokens to pay for goods and services, giving tokens away to another person and exchanging tokens for another kind of cryptoasset.

- Companies that account for exchange tokens as "intangible assets" may be taxed under CT rules for intangible fixed assets if the token is both an "intangible asset" for accounting purposes and an "intangible fixed asset". This requires that the relevant exchange token has been created or acquired by a company for use on a continuing basis. Exchange tokens that are simply held by the company, even when held in the course of its activities, will not meet this definition. If these conditions are met, the CT rules for intangible fixed assets (Corporation Tax Act 2009 Part 8) have priority over the chargeable gains rules.
- A company has a "loan relationship" if it has a money debt that has arisen from a transaction for the lending of money. HMRC does not consider exchange tokens to be money. In addition, there is typically no counterparty standing behind the token; as such, the token does not seem to constitute a debt. This means that exchange tokens do not create a loan relationship. If exchange tokens have been provided as collateral security for an ordinary loan (of money), a loan relationship exists, and the loan relationship rules will apply (whether the company is the debtor or creditor).
- Value-added tax ("**VAT**") is due in the normal way on any VAT-able goods or services sold in exchange for exchange tokens. The value of the supply of goods or services on which VAT is due will be the pound sterling value of the exchange tokens at the point the transaction takes place. However, no VAT will be due on the supply of the token itself (despite HMRC's prevailing view that cryptocurrencies are not currency or money for direct tax purposes). In addition, the exchange of traditional currencies for non-legal tender such as Bitcoin (and *vice versa*), as well as a supply of any services required for this type of exchange, constitute financial transactions that are exempt from VAT.
- Stamp duty and stamp duty reserve tax ("**SDRT**") will not usually be chargeable on the transfer of exchange tokens. HMRC's view is that existing exchange tokens are unlikely to meet the required definition of "stock or marketable securities" or "chargeable securities". However, each exchange token will need to be considered on its own facts and circumstances in the context of the definitions of "stock or marketable securities" or "chargeable securities".
- In terms of exchange tokens being given as consideration for purchases of "stock or marketable securities" or "chargeable securities", SDRT requires that chargeable consideration is "money or money's worth". Exchange tokens constitute "money's worth" and are therefore chargeable for SDRT purposes.
- Stamp duty land tax ("**SDLT**") will not be payable on transfers of exchange tokens, since HMRC does not consider such transfers to be land transactions. As with SDRT, chargeable consideration for SDLT purposes includes anything given for the transaction that is "money or money's worth". Accordingly, 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 SDLT.

Money transmission laws and anti-money laundering requirements

Money transmission laws

The principal UK laws relevant to money transmission are the PSRs and EMRs. Together, the PSRs and EMRs establish a regulatory framework applicable to persons performing payment services (including, for example, money remittance) and issuing electronic money in the UK, which includes authorisation, organisational, regulatory capital, safeguarding and conduct of business requirements. Whether this framework applies depends on whether a service involves payment services or the issue of electronic money as defined by the PSRs and EMRs, respectively.

Payment services as defined by the PSRs necessarily involve funds. Cryptocurrencies are generally not considered funds for these purposes. Therefore, products and services involving only cryptocurrency (such as a crypto-to-crypto exchange) will not normally involve payment services. Important exceptions are products or services relating to what the FCA Guidance terms "e-money tokens". Take, for example, a stablecoin structured in a way that means it constitutes electronic money – issuing such a stablecoin would likely trigger the application of the EMRs, and providing wallet services in relation to such a stablecoin would likely trigger the application of the PSRs (since electronic money is a form of funds for the purposes of the PSRs).

Conversely, where fiat currency is involved (e.g., in the context of a fiat-to-crypto exchange) there will be funds, and so further analysis would need to be conducted to determine whether payment services are being provided and, if so, the precise application of the regulatory regime established by the PSRs.

Anti-money laundering requirements

UK AML requirements are principally contained in the Money Laundering, Terrorist Financing and Transfer of Funds (Information on the Payer) Regulations 2017 ("**MLRs**").

The MLRs implement the Fourth EU Money Laundering Directive in the UK and impose various requirements on businesses that are within their scope, including: the requirement to perform a firm-level AML risk assessment; organisational requirements relating to AML (including systems and controls and record-keeping requirements); customer due diligence obligations when establishing a business relationship with a customer or when transacting above a certain threshold; and ongoing monitoring obligations. The MLRs only apply to those businesses that have been identified as the most vulnerable to the risk of being used for money laundering or terrorist financing.

On 10 January 2020, the MLRs were amended to incorporate the Fifth EU Money Laundering Directive ("**MLD5**") into UK law. This change brought cryptoasset exchange providers ("**CEPs**") and custodian wallet providers ("**CWPs**") within the scope of the MLRs. As such, the MLRs impact any person conducting cryptoasset business of a kind that is captured by the new definitions of CEP or CWP in the UK (including, for example, existing UK authorised financial services firms that carry on relevant cryptoasset business).

For the purposes of the MLRs, CEPs, CWPs and cryptoassets are defined as follows:

- CEP: "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, when providing such services—
  (a) exchanging, or arranging or making arrangements with a view to the exchange of, cryptoassets for money or money for cryptoassets,
  (b) exchanging, or arranging or making arrangements with a view to the exchange of, one cryptoasset for another, or
  (c) operating a machine which utilises automated processes to exchange cryptoassets for money or money for cryptoassets."
- CWP: "a firm or sole practitioner who by way of business provides services to safeguard, or to safeguard and administer—
  (a) cryptoassets on behalf of its customers, or
  (b) private cryptographic keys on behalf of its customers in order to hold, store and transfer cryptoassets,
  when providing such services."

- Cryptoasset: "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."

Significantly, a person may be a CEP or CWP regardless of whether they are otherwise regulated in the UK if they carry on cryptoasset business of a kind that is captured by the new definitions. As such, the requirements relating to cryptoasset business in the MLRs apply to both regulated and unregulated cryptoasset businesses in the UK. Notably, the definition of a CEP goes beyond the requirements of MLD5, capturing crypto-to-crypto exchange (in addition to crypto-to-fiat exchange). The CEP definition may also capture market participants that would not ordinarily be regarded as exchanges in the strict sense. For example, cryptoasset brokers that buy and sell cryptoassets for their customers or for their own account when executing client orders are likely to be captured by the definition, in addition to exchanges that facilitate interactions between buyers and sellers of cryptoassets. Issuers of cryptoassets may also be captured in certain circumstances.

Typically, providers of non-custodial cryptoasset wallet software will not be captured by the CWP definition.

CEPs and CWPs are required to register with the FCA before carrying on relevant cryptoasset business in the UK. The FCA clarified that existing UK authorised persons (including existing UK banks, investment firms, electronic money institutions and payment services businesses) undertaking relevant cryptoasset business must apply for registration. Registration must be completed via the FCA's online system, Connect, and applicants must provide a significant amount of information relating to their business and all staff who hold relevant functions to allow the FCA to assess whether or not the applicant is fit and proper. An applicant for registration must provide various information, including: a programme of operations; a business plan; a description of the applicant's structural organisation; a detailed guide to the applicant's IT systems and controls; and details of relevant individuals, beneficial owners and close links.

In addition to the ordinary AML requirements that apply generally to businesses within the scope of the MLRs (including CEPs and CWPs), there is a specific additional requirement that a business whose relevant cryptoasset activity does not fall within the scope of the Financial Ombudsman Service or the Financial Services Compensation Scheme must inform its customers of this fact before entering into a relevant business relationship or transaction. There are also specific reporting requirements that apply to CEPs and CWPs (see *Reporting requirements* below).

Relatedly, the Joint Money Laundering Steering Group[23] published sector-specific guidance relating to cryptoasset business in July 2020. The guidance clarified the scope of the MLRs in relation to cryptoassets, discussed the money laundering and terrorist financing risks pertinent to the sector, assessed these risks and provided guidance on how CEPs and CWPs might interpret the AML requirements under the MLRs (e.g., customer due diligence, transaction analysis, record-keeping and sanctions screening) as would be appropriate to the cryptoasset sector.

At the time of writing, HM Treasury is consulting[24] on the extension of the so-called "travel rule" (the requirement for financial institutions to send and record information on the originator and beneficiary of a wire transfer, and for this information to remain with the transfer or related message throughout the payment chain) to CEPs and CWPs. In its consultation, HM Treasury states that the government considers that "the time is now right" to begin planning for the implementation of the travel rule to cryptoasset transfers (tailored

where appropriate to reflect the nature of the underlying technology involved), after previously deciding to defer the implementation of the travel rule for such transfers in order to allow compliance solutions to be developed. However, the consultation acknowledges that "the process of integrating these requirements into a firm's business practices may take time", and that the government therefore proposes to allow firms a grace period after the amendments to the AML regime are made, to allow for the integration of compliance solutions. The length of this proposed grace period is not set out in the consultation, and respondents are invited to give their views on how long it should be. Legislation giving effect to the relevant changes is currently expected to be introduced in Spring 2022.

Promotion and testing

In November 2018, the FCA established an Innovation Division, which encompasses initiatives that the regulator has developed in recent years relating to innovation in financial services. Notably, the following areas fall under the Innovation Division in relation to promotion and testing:

- *The FCA's Regulatory Sandbox*, which allows both authorised and unauthorised businesses that meet certain eligibility criteria to test innovative financial services propositions in the market with real consumers. Firms that successfully apply to participate in the Sandbox may benefit from the various Sandbox "tools" that the FCA can deploy to facilitate real-world testing, such as restricted authorisation, individual guidance, informal steers, waivers and no-enforcement action letters.
- *The Global Financial Innovation Network*, which grew out of the FCA's proposal to create a global Sandbox. The Network seeks to provide a more efficient way for innovative firms to interact with regulators, helping them navigate between countries as they look to scale new ideas. The Network is for firms wishing to test innovative products, services or business models across more than one jurisdiction.
- *The FCA's Innovation Hub*, which offers direct support from the FCA to eligible innovative businesses by providing a dedicated contact for businesses that are considering applying for authorisation or a variation of permission, need support when doing so, or do not need to be authorised but could benefit from FCA support.

Ownership and licensing requirements

In the interests of improving legal certainty with respect to ownership and transfer of cryptoassets, the England and Wales Law Commission is in the process of consulting[25] on digital assets. The Law Commission's work will involve surveying the current state of English private law (i.e., not including regulatory, taxation, data protection, criminal, settlement finality or AML issues) relating to digital assets, as well as making recommendations as to possible changes to such law with respect to digital assets. The focus of the Law Commission's work is therefore on questions such as: whether and how cryptoassets can be characterised as personal property; whether cryptoassets should be amenable to concepts such as possession and bailment; whether and how security interests may be granted over cryptoassets; and how cryptoassets should be treated for the purposes of UK insolvency law. In this regard, the Law Commission endorses and intends to build on the Legal Statement[26] published by the UK Jurisdiction Taskforce ("**UKJT**") of the UK government's LawTech Delivery Panel in November 2019 covering similar topics. In its Legal Statement, the UKJT concluded that cryptoassets are capable of having all the legal characteristics of property under English law and are therefore capable of being treated as a form of property. Indeed, since the publication of the Legal Statement (which in itself is

not legally binding), it has been adopted by the High Court of England and Wales, which has held in more than one case that particular cryptoassets were capable of being a form of property.[27] The Law Commission also starts from the premise that the law will treat certain cryptoassets as property, where those cryptoassets satisfy the legal characteristics of property under English law.

As to licensing requirements, whether or not a person requires authorisation to perform their activities in relation to cryptocurrencies in the UK will depend on whether they are conducting "regulated activities" as defined by FSMA, or payment services/e-money activities that require authorisation under the PSRs or EMRs. The registration requirement for cryptoasset businesses under the MLRs must also be kept in mind. As noted in *Cryptocurrency regulation* above, a person's activities in relation to cryptocurrencies may still be subject to UK financial regulation even where the underlying cryptocurrency involved is not a specified investment. For example, establishing, operating, marketing or managing a fund that offers exposure to unregulated cryptocurrencies by way of business is the kind of activity that may well trigger licensing requirements in the UK. For the time being, cryptocurrencies are also unlikely to be permissible for inclusion in fund products (e.g., exchange-traded funds) that require approval from the FCA: the Taskforce Report makes clear that the FCA will not authorise or approve the listing of a transferable security or fund that references exchange tokens unless it has confidence in the integrity of the underlying market and that other regulatory criteria for funds authorisation are met.

Mining

Mining cryptocurrencies is permitted in the UK, and as noted above, there is no bespoke financial regulatory regime for cryptocurrencies in the UK that expressly regulates this activity. Mining of cryptocurrencies is also unlikely to fall within the existing UK financial regulatory perimeter (e.g., mining Bitcoin is not currently subject to UK financial regulation).

Border restrictions and declaration

There are currently no border restrictions or requirements to declare cryptocurrency holdings when entering the UK. Individuals carrying cash in excess of EUR or GBP 10,000 must declare this to HMRC upon entering the UK from certain countries, but cryptocurrencies are not regarded as cash for these purposes.

Reporting requirements

Depending on the nature of the cryptoasset and the business activity in question, general reporting requirements that arise as a result of existing financial regulation (e.g., transaction reporting) or AML legislation (e.g., the requirement to submit suspicious activity reports to the National Crime Agency) could apply in relation to cryptocurrency transactions.

In addition, the MLRs now contain a broad reporting requirement that applies to CEPs and CWPs, under which they must provide to the FCA "such information as the FCA may direct" relating to compliance with the MLRs or that is "otherwise reasonably required by the FCA in connection with the exercise by the FCA of any of its supervisory functions". Such reports must be made "at such times and in such form, and verified in such manner, as the FCA may direct". The FCA has consulted on[28] and extended[29] to CEPs and CWPs the requirement to provide an annual financial crime report, which previously only applied to certain authorised firms. Otherwise, no guidance has been forthcoming as to how the FCA intends to utilise its powers in relation to reporting by CEPs and CWPs under the MLRs, and so it remains to be seen what kinds of reports the FCA will require in this regard.

Estate planning and testamentary succession

There are no specific rules as to how cryptocurrencies are treated for the purposes of estate planning and testamentary succession; therefore, the normal relevant legal principles apply. Consequently, cryptocurrencies are likely to fall within the broad definition of property for the purposes of inheritance tax[30] and will likely be subject to taxation should a chargeable transfer arise. Prior to death, a testator will need to instruct their personal representative on how to obtain the relevant cryptographic keys and details of the wallet service provider (where relevant), as without such means of dealing with the cryptocurrency it will be rendered effectively worthless.

* * *

Endnotes

1. *Cryptoassets Taskforce: Final Report* (26 October 2018) https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/752070/cryptoassets_taskforce_final_report_final_web.pdf (accessed 27 September 2021).
2. *Final Report* (n 1), 2.10.
3. *Ibid.*, 2.11.
4. For example, at the time of writing, both the FCA and Bank of England websites warn that anyone investing in cryptoassets (including cryptocurrencies) should be aware that they are very risky, volatile investments and should be prepared to lose all of the money invested https://www.fca.org.uk/consumers/cryptoassets, https://www.bankofengland.co.uk/KnowledgeBank/what-are-cryptocurrencies (accessed 27 September 2021).
5. FCA, *CP19/3: Guidance on Cryptoassets* (23 January 2019) https://www.fca.org.uk/publication/consultation/cp19-03.pdf (accessed 27 September 2021).
6. FCA, *PS19/22: Guidance on Cryptoassets* (31 July 2019) https://www.fca.org.uk/publication/policy/ps19-22.pdf (accessed 27 September 2021).
7. FCA, *CP19/22: Prohibiting the sale to retail clients of investment products that reference cryptoassets* (3 July 2019) https://www.fca.org.uk/publication/consultation/cp19-22.pdf (accessed 27 September 2021).
8. FCA, *PS20/10: Prohibiting the sale to retail clients of investment products that reference cryptoassets* (6 October 2020) https://www.fca.org.uk/publication/policy/ps20-10.pdf (accessed 27 September 2021).
9. "We have not yet made a decision on whether to introduce CBDC." Bank of England website https://www.bankofengland.co.uk/research/digital-currencies (accessed 27 September 2021).
10. Bank of England, *Central Bank Digital Currency – opportunities, challenges and design* (March 2020) https://www.bankofengland.co.uk/-/media/boe/files/paper/2020/central-bank-digital-currency-opportunities-challenges-and-design.pdf?la=en&hash=DFAD18646A77C00772AF1C5B18E63E71F68E4593, https://www.bankofengland.co.uk/news/2021/april/bank-of-england-statement-on-central-bank-digital-currency (accessed 27 September 2021).
11. As set out here: https://www.fca.org.uk/firms/cryptoassets (accessed 27 September 2021).
12. https://www.fca.org.uk/firms/cryptoassets (accessed 27 September 2021).
13. This is consistent with the approach taken in the FCA Guidance. See, for example, paragraphs 42, 45, 49 and 65 to 67 of the FCA Guidance: *PS19/22* (n 6), Appendix 1.
14. *PS19/22* (n 6), Appendix 1 41.

15. *Ibid.*, 43 to 44.
16. HM Treasury, *UK regulatory approach to cryptoassets and stablecoins: consultation and call for evidence* (7 January 2021) https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/950206/HM_Treasury_Cryptoasset_and_Stablecoin_consultation.pdf (accessed 27 September 2021).
17. The FCA maintains a list of UK regulated markets https://register.fca.org.uk/s/search?predefined=RM (accessed 27 September 2021).
18. Electronic money does not fall within the definition of transferable securities.
19. HM Treasury, *Regulatory framework for approval of financial promotions: consultation* (20 July 2020) https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/902101/Financial_Promotions_Unauthorised_Firms_Consultation.pdf (accessed 27 September 2021).
20. HM Treasury, *Cryptoasset promotions – consultation* (20 July 2020) https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/902891/Cryptoasset_promotions_consultation.pdf (accessed 27 September 2021).
21. HMRC, *Cryptoassets for individuals* (19 December 2019) https://www.gov.uk/government/publications/tax-on-cryptoassets/cryptoassets-for-individuals (accessed 27 September 2021).
22. HMRC, *Cryptoassets for businesses* (20 December 2019) https://www.gov.uk/government/publications/tax-on-cryptoassets/cryptoassets-tax-for-businesses (accessed 27 September 2021).
23. JMLSG, *Guidance for the UK financial sector – Part II: sectoral guidance* (amended July 2020) https://secureservercdn.net/160.153.138.163/a3a.8f7.myftpupload.com/wp-content/uploads/2020/07/JMLSG-Guidance_Part-II_-July-2020.pdf (accessed 27 September 2021).
24. HM Treasury, *Amendments to the Money Laundering, Terrorist Financing and Transfer of Funds (Information on the Payer) Regulations 2017 Statutory Instrument 2022: consultation* (22 July 2021) https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/1004603/210720_SI_Consultation_Document_final.pdf (accessed 27 September 2021).
25. Law Commission, *Digital assets: call for evidence* (30 April 2021) https://s3-eu-west-2.amazonaws.com/lawcom-prod-storage-11jsxou24uy7q/uploads/2021/04/Call-for-evidence.pdf (accessed 27 September 2021).
26. UK Jurisdiction Taskforce, *Legal Statement on cryptoassets and smart contracts* (November 2019) https://35z8e83m1ih83drye280o9d1-wpengine.netdna-ssl.com/wp-content/uploads/2019/11/6.6056_JO_Cryptocurrencies_Statement_FINAL_WEB_111119-1.pdf (accessed 27 September 2021).
27. *AA v Persons Unknown* [2019] EWHC 3556 (Comm) (17 January 2020); *Ion Science Ltd v Persons Unknown* (unreported, 21 December 2020).
28. FCA, *CP20/17: Extension of Annual Financial Crime Reporting Obligation* (24 August 2020) https://www.fca.org.uk/publication/consultation/cp20-17.pdf (accessed 27 September 2021).
29. FCA, *PS21/4: Extension of Annual Financial Crime Reporting Obligation* (31 March 2021) https://www.fca.org.uk/publication/policy/ps21-4.pdf (accessed 27 September 2021).
30. HMRC, *Inheritance Tax Manual: structure of the charge: what is property?* (updated 14 September 2021) https://www.gov.uk/hmrc-internal-manuals/inheritance-tax-manual/ihtm04030 (accessed 27 September 2021).

Stuart Davis
Tel: +44 20 7710 1821 / Email: stuart.davis@lw.com

Stuart Davis is a partner in the London office of Latham & Watkins and a member of the FinTech Industry Group. Mr. Davis has a wide range of experience advising broker-dealers; investment, retail, and private banks; technology companies; market infrastructure providers; investment managers; hedge funds; and private equity funds on complex regulatory challenges.

Mr. Davis counsels clients on the domestic and cross-border regulatory aspects of cutting-edge FinTech initiatives, including technology innovations in legislation, market infrastructure, tokenisation, trading, clearing and settlement, lending (including crowdfunding), payments, and regulatory surveillance. He also advises financial institutions on the impact of regulatory change on their businesses, including MAR and MiFID II, CASS, CSDR, PSD2, AIFMD, and Brexit, as well as strategically advising on their FX remediation projects, market conduct issues, best execution compliance, systems and controls, and governance.

Sam Maxson
Tel: +44 20 7710 1823 / Email: sam.maxson@lw.com

Sam Maxson is an associate and a member of the FinTech Industry Group in the London office of Latham & Watkins.

Mr. Maxson regularly advises a wide range of clients (including banks, insurers, investment firms, financial markets infrastructure providers, and technology companies) on all aspects of financial regulation. Mr. Maxson has a particular focus on FinTech and InsurTech, advising both established and emerging businesses on the application of global financial regulation to new and novel uses of technology in finance and insurance. His experience also encompasses the increasingly widespread interest in cryptoassets and the "tokenisation" of financial markets.

Andrew Moyle
Tel: +44 20 7710 1078 / Email: andrew.moyle@lw.com

Andrew Moyle is the Global Co-Chair of Latham & Watkins' FinTech Industry Group and a partner in the London office. He has more than 20 years of experience in providing commercial legal advice on the structuring, negotiation, implementation, and management of complex technology and outsourcing transactions. Mr. Moyle advises clients ranging from traditional financial institutions to new technology incumbents on the "tech" in FinTech, including on payments and transfers, InsurTech, and virtual currencies.

In his broader technology practice, Mr. Moyle advises clients on commercial contracts and collaborations, cloud computing, outsourcing, digital and disruptive technology, telecommunications technology, and enterprise systems. He regularly engages as the lead legal advisor on outsourcing programs, strategic sourcing functions, and transformation initiatives. In addition to financial services, he also advises clients in the leisure, energy, retail, and natural resource sectors.

Latham & Watkins

99 Bishopsgate, London EC2M 3XF, United Kingdom
Tel: +44 20 7710 1000 / Fax: +44 20 7374 4460 / URL: www.lw.com

USA

Josias N. Dewey
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 and the Department of 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.

Several 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 has been praised for becoming the most crypto-friendly jurisdiction in the country. Another state, Colorado, passed a bipartisan bill exempting cryptocurrencies from state securities regulations. Ohio became the first U.S. state to start accepting taxes in cryptocurrency. Oklahoma introduced a bill authorizing cryptocurrency to be used, offered, sold, exchanged and accepted as an instrument of monetary value within its governmental agencies. On the other hand, Iowa introduced a bill that would prohibit the state and political subdivisions of the state from accepting payment in the form of cryptocurrencies. Authorities in at least 10 other states, like Maryland and Hawaii, have issued warnings about investing in cryptocurrencies. New York, which passed laws once considered restrictive, has eased restrictions for attaining a BitLicense in the hopes of luring back cryptocurrency companies that previously exited the New York market.

There is no uniform definition of "cryptocurrency," which is often referred to as "virtual currency," "digital assets," "digital tokens," "cryptoassets" or simply "crypto." While some

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.

Cryptocurrency regulation

This is discussed in detail below.

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. In addition, the CFTC has jurisdiction over attempts to engage in market manipulation with respect to those cryptoassets that are considered commodities. The likelihood of the CFTC asserting its authority to prevent market manipulation is much higher today as a result of both the CBOE and the CME offering futures linked to the price of Bitcoin.

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. 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 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.

The outcome of the Telegram and Kik proceedings has made 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 Regulation S safe harbor). With little prospect of legislative action, the hostile environment towards token-generating events in the U.S. is likely to continue for the foreseeable future.

In addition to Federal securities laws, most states have their own laws, referred to as blue sky laws, which are not always preempted by Federal law. Anyone selling digital assets likely to constitute a security should check with counsel about the applicability of blue sky laws. Of particular importance, there are certain exemptions from registration under Federal law that do not preempt the application of state blue sky laws.

It is worth noting that state securities regulators increased their scrutiny of digital assets during 2021. An area of particular focus has been exchanges and others offering interest-bearing crypto accounts. New Jersey and several other states issued cease and desist orders against BlockFi, a well-known crypto exchange, for offering such interest-bearing accounts.

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 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 harmonizing traditional securities laws around the transfer of securities and the notion of a peer-to-peer network that seeks to operate without intermediaries.

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 U.S. Department 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 Department issued a correspondence that called into question whether ICO issuers were *de facto* an MSB that was 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 USD, 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 decentralized finance ("**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 two 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 amongst the cryptocurrency community. During August 2021, over $40 billion of transactions occurred using the Uniswap Protocol. In September 2021, it was reported that the SEC had begun an investigation into Uniswap Labs and its Uniswap Protocol.

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), which 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.

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, Utah, 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.

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 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, Ether, Litecoin, 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 less than 100 beneficial owners.

Regardless of whether a startup cryptocurrency fund manager is required to register as a CTA/CPO 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 general rule of thumb regarding Bitcoin mining remains relatively straightforward. If you are able to own and use cryptocurrency where you live, you should also be able to mine cryptocurrency in that location as well. If owning cryptocurrency is illegal where you live, mining is most likely also illegal. There are few, if any, jurisdictions in the U.S. where possession of cryptocurrency is illegal. Plattsburgh, New York, however, is likely the only city in the U.S. to impose a ban (temporary) on cryptocurrency mining. Also, the U.S. Marine Corps banned crypto mining apps from all government-issued mobile devices.

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

We are not aware of any broadly applicable reporting requirements specific to cryptocurrency in the U.S.

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, if you want greater certainty of bequeathing cryptocurrency to your heirs, you will need to provide specific and detailed written instructions in your estate planning documents. The information you will need to include will depend upon the type of virtual currency wallet you 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*".

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

Other titles in the **Global Legal Insights** series include:

AI, Machine Learning & Big Data
Banking Regulation
Bribery & Corruption
Cartels
Corporate Tax
Employment & Labour Law
Energy
Fintech
Fund Finance
Initial Public Offerings
International Arbitration
Litigation & Dispute Resolution
Merger Control
Mergers & Acquisitions
Pricing & Reimbursement

GLI GLOBAL LEGAL INSIGHTS