TOKEN ALLIANCE

CHAMBER OF DIGITAL COMMERCE

SECOND EDITION

Understanding Digital Tokens:

Market Overviews and Guidelines for Policymakers and Practitioners

Prepared by the Token Alliance – an industry initiative of the Chamber of Digital Commerce

JANUARY 2020

CHAMBER OF DIGITAL COMMERCE

The Chamber of Digital Commerce is the world's largest trade association representing the blockchain industry. Our mission is to promote the acceptance and use of digital assets and blockchain technology. Through education, advocacy, and working closely with policymakers, regulatory agencies, and industry, our goal is to develop a pro-growth legal environment that fosters innovation, jobs, and investment.

TOKEN ALLIANCE

The Token Alliance is an industry-led initiative of the Chamber of Digital Commerce, developed to be a key resource for the emerging industry surrounding the generation and distribution of tokens using blockchain technology. Comprised of more than 400 industry participants, the Alliance includes blockchain and token legal experts, technologists, economists, former regulators, and practitioners from around the globe. The Token Alliance develops community-driven guidelines for the responsible development of tokens.

CHAMBER OF DIGITAL COMMERCE INDUSTRY INITIATIVES & WORKING GROUPS

SMART CONTRACTS ALLIANCE

Promotes real-world application of smart contracts to enhance the way business is conducted.

GLOBAL BLOCKCHAIN FORUM

Working with the world's leading blockchain policy experts to develop industry best practices and help shape global regulatory interoperability.

BLOCKCHAIN ALLIANCE

The public-private forum for the blockchain community and law enforcement to help combat criminal activity.

BLOCKCHAIN INTELLECTUAL PROPERTY COUNCIL

Balancing the protection of proprietary information with the openness necessary for innovation.

DIGITAL ASSETS ACCOUNTING CONSORTIUM

Developing accounting and reporting standards for digital assets and blockchain-based technologies.

STATE WORKING GROUP

Engaging with state and local governments on the regulation and implementation of blockchain technology.

CHAMBER OF DIGITAL COMMERCE CANADA

Promoting the acceptance and use of digital assets and blockchain-based technologies in Canada.

TABLE OF CONTENTS

I. ACKNOWLEDGEMENTS

TOKEN ALLIANCE CO-CHAIRS

PAUL ATKINS

Chief Executive Officer, Patomak Global Partners
Non-Executive Chairman, BATS Global Markets, Inc. (2012-2015)
Commissioner, U.S. Securities and Exchange Commission (2002-2009)

JAMES NEWSOME, PH.D.

Founding Partner, Delta Strategy Group
President & CEO, New York Mercantile Exchange (2004-2008)
Chairman, U.S. Commodity Futures Trading Commission (2001-2004)
Commissioner, U.S. Commodity Futures Trading Commission (1998-2001)

TOKEN ALLIANCE LEADERSHIP COMMITTEE

The Chamber of Digital Commerce would like to recognize the following individuals for their thought leadership, contributions and support to the Token Alliance in the production of this report.

KEVIN BATTEH
Partner,
Delta Strategy Group

PERIANNE BORING
Founder and President,
Chamber of Digital Commerce

JOE CUTLER
Partner,
Perkins Coie LLP

DAX HANSEN
Partner,
Perkins Coie LLP

CHRIS HOUSSER
Co-Founder,
Polymath

JONATHAN JOHNSON
President,
Medici Ventures

AMY DAVINE KIM
Chief Policy Officer,
Chamber of Digital Commerce

KARI LARSEN
Partner,
Perkins Coie LLP

BRIAN LIO
Chief Executive Officer,
Smith + Crown

RUMI MORALES
Partner,
Outlier Ventures

MATTHEW ROSZAK
Chairman and Co-Founder,
Bloq

BILL SHIHARA
Chief Executive Officer,
Bittrex

TOM SPORKIN
Partner, Buckley LLP
Strategic Advisor, Token Alliance

JOSHUA STEIN
Chief Executive Officer,
Harbor

COLLEEN SULLIVAN
Chief Executive Officer,
CMT Digital

TOKEN ALLIANCE

CHAMBER OF DIGITAL COMMERCE

UNDERSTANDING DIGITAL TOKENS

Considerations and Guidelines for Securities and Non-Securities Tokens

Prepared by the Token Alliance – an industry initiative of the Chamber of Digital Commerce

SECOND EDITION • AUGUST 2019

CONSIDERATIONS AND GUIDELINES FOR SECURITIES AND NON-SECURITIES TOKENS

The Chamber of Digital Commerce would like to thank the following individuals and organizations for their valuable contributions to the Token Alliance in the production of this report.

We would also like to extend a special thank you to **Matthew Comstock of Murphy & McGonigle** for helping to lead the development of this report.

CHAPTER 1

THOMAS AHMADIFAR
Perkins Coie

DAVID AKTARY
ERC dEX

KRISTIN BOGGIANO
AlphaPoint

PAUL BRIGNER
Chamber of Digital Commerce

MATT CHWIERUT
Smith + Crown

LEWIS COHEN
DLx Law

BRIAN CRUMP
Much Law

MIKE DIDIUK
Perkins Coie

BRANDT DOWNES
Smith + Crown

ERIC FREDELL
Chamber of Digital Commerce

FREDERICK FEDYNYSHYN
Perkins Coie

TROY FOSTER
Perkins Coie

JOEY GARCIA
ISOLAS

GREG GROVE
Much Law

STEVE HOPKINS
tZERO Group

JONATHAN IP
RockTree Capital

ALAN KONEVSKY
tZERO Group

KRISTINE LAVEAU
Much Law

BEN LIM
Debevoise & Plimpton

BRIAN LIO
Smith + Crown

COLIN LLOYD
Cleary Gottlieb

RICHARD MA
Quantstamp

OLGA MACK
Quantstamp

GARY MURPHY
Debevoise & Plimpton

LINDSAY NELSON
Smith + Crown

OMER OZDEN
RockTree Capital

DIVIJ PANDYA
Chamber of Digital Commerce

ARABY PATCH
Securitize

ERIC SIBBITT
O'Melveny & Myers

WILLIAM SONG
RockTree Capital

COLLEEN SULLIVAN
CMT Digital

CHAPTER 2:

THOMAS AHMADIFAR
Perkins Coie

STEVE BUNNELL
Bittrex

MATT CHWIERUT
Smith + Crown

LEWIS COHEN
DLx Law

MICHAEL DIDIUK
Perkins Coie

FREDERICK FEDYNYSHYN
Perkins Coie

DROR FUTTER
Rimon Law

PARITOSH GAMBHIR
KPMG

GREGORY GROVE
Much Law

KATE GUIMBELLOT
TravelCoin Foundation

SHARON HAVERLAH
USAA

RAMON LAFEE
G Coin

STEPHEN KEEN
Perkins Coie

JAY NATARAJAN
Microsoft

KWON PARK
Bittrex

SCOTT PARSONS
Delta Strategy Group

KIRAN RAJ
Bittrex

ERIC SIBBITT
O'Melveny & Myers

J. GRAY SASSER
Frost Brown Todd

STEVEN SPRAGUE
Rivetz

JASON WEINSTEIN
Steptoe

LES WILKINSON
Hashed Health

TABLE OF CONTENTS

II. INTRODUCTION

This new installment of our series of reports is an important addition to the overall regulatory and market consideration of the token ecosystem. The way in which digital tokens operate is complex and can maintain multiple characteristics – from an investment contract, to something necessary for utilizing a digital platform, to a form of payment or exchange, to name just a few. We are in a moment when technological advancement is pushing the boundaries of decades-long established law – law that was made at a time when tokenized assets and instantaneous digital transfers of value were not contemplated. It is exciting to be a part of it, but it also entails risks.

To facilitate the development of token businesses as well as minimize incidents of fraud and compliance challenges, the Chamber embarked on a plan to tackle each of the issues impacting this ecosystem. This journey started with a publication of guidelines for digital tokens that were intended to operate outside Securities and Exchange Commission (SEC) and Commodities Futures Trading Commission (CFTC)-regulated products and services laws (so-called "utility tokens" and associated platforms).

Those Guidelines also sought to provide legal context by detailing the legal landscapes governing digital tokens in five countries – the United States, Canada, the United Kingdom, Australia, and Gibraltar. Taking up a sizeable portion of the Report, the description of the vast number of potential legal requirements and government oversight demonstrated that this is a regulated industry, no matter where you fall in the spectrum of token categorization.

Finally, we provided an economic perspective on the industry with an analysis of market trends. The sheer volume of capital raised demonstrates the passionate interest of so many around the world in the potential of these markets – whether as a way to make money, a way to use new and better services, or other reasons.

This installment expands on those initial resources to balance out the conversation around utility tokens to discuss the rules, regulations, and resulting considerations for those who wish to issue or trade tokens that are or otherwise represent securities. This sector of the market is growing with entrants from new technology companies as well as established institutional financial services providers. The securities laws are complex, generated in the 1930s and developing substantial legal and regulatory precedent. In some cases, that precedent has endured because it is principles-based. In others, it has become outdated as it no longer sufficiently contemplates the types of securities that can be created, issued, held, and traded digitally.

We are excited to introduce these guidelines for securities tokens to complement our work involving utility tokens. But we can't stop there. More areas need to be considered and addressed with thoughtful analysis. In the coming days and weeks, we also intend to publish guidelines around cyber security, consumer protection, and anti-money laundering. We will be supplementing our legal landscape on a rolling basis with the introduction of additional countries and the laws that apply to digital tokens. And finally, the market has had its ups and downs since the publication of our first Report. Smith + Crown will provide an update on trends, facts, and figures to better understand the scope of this growing evolution.

We hope you enjoy these publications and that they serve to help guide your analysis and views of the evolving digital token ecosystem. We look forward to sharing this series as we roll out these publications throughout the coming weeks!

A few words of caution:

THIS REPORT DOES NOT CONSTITUTE LEGAL ADVICE

- Specifically, nothing in this report should be construed as advice regarding the law of the United States or any other jurisdiction.
- This report's analysis of the criteria under which it is determined that tokens constitute securities or commodities do not constitute a restatement of law.
- This report, including its suggested guidelines, merely express the general views of the Token Alliance, and compliance with such guidelines cannot assure that the distribution or trading of tokens will fully comply with the laws discussed herein.
- These views are being offered for discussion purposes only, and they have not been sanctioned by the SEC, CFTC, or any other regulator or government agency.

CONSULT LEGAL COUNSEL BEFORE DISTRIBUTING OR HOSTING TRADES OF DIGITAL TOKENS

- Token Sponsors and associated parties seeking to generate or distribute a blockchain-based token should seek independent legal counsel with expertise in this area before proceeding with their project, particularly given the fast-paced nature of this industry and the quickly evolving legal landscape.
- Counsel can help consider the facts and circumstances surrounding particular issues within the contours of then-current regulatory and enforcement activity.
- This report does not attempt to address any individual case, and the thought leadership contained herein is not appropriate for use as a substitute for independent counsel.
- Further, the digital token market is rapidly shifting and therefore the cases and regulatory interpretations discussed in this report may be overtaken by future events.

The Token Alliance will continue to study the issues surrounding the appropriate regulation for tokens and it will offer additional insights, as appropriate, when new developments arise.

III. CHAPTER 1: CONSIDERATIONS AND GUIDELINES FOR SECURITIES TOKENS

I. INTRODUCTION

This paper describes the application of the securities laws, regulations, and rules of the United States to the issuance and trading of "tokenized securities" as that term is defined below. Tokenized securities, like other securities, are subject to the jurisdiction of the U.S. Securities and Exchange Commission ("SEC") but are different from other securities in that they apply blockchain technology to raise funds, track ownership, and deliver value to securities holders.

A "tokenized security" is a cryptographic token[1] built on a blockchain[2] (or distributed ledger) which represents or symbolizes an instrument that meets the definition of a "security"[3] under Section 2(a)(1) of the Securities Act of 1933, as amended (the "Securities Act"), including an "investment contract" as interpreted by the Supreme Court in *SEC v. W.J. Howey Co.*[4] In contrast to protocol or utility tokens, which typically are sold for consumptive use on a blockchain network, tokenized securities are issued to be securities within the meaning of the Securities Act. Tokenized securities are therefore securities with an "electronic wrapper," which enables new and evolving functionality and the ability to be traded on both public and private blockchains.

TOKENIZED SECURITY

Cryptographic token which is, represents, or symbolizes an instrument that meets the definition of a "security."

UTILITY TOKENS

Allows a holder to consume or redeem the token for a good or service in a functioning system, or a cryptocurrency token on a blockchain network.

1 Digital tokens are computer code maintained on a blockchain-based ledger that are secured using cryptography, with each token typically representing a specific value or amount on the ledger.

2 A blockchain is a specific type of distributed ledger technology that organizes data into blocks that are "chained" together chronologically by a cryptographic hash function and confirmed by a consensus mechanism.

3 "The term "security" means any note, stock, treasury stock, security future, security-based swap, bond, debenture, evidence of indebtedness, certificate of interest or participation in any profit-sharing agreement, collateral-trust certificate, preorganization certificate or subscription, transferable share, investment contract, voting-trust certificate, certificate of deposit for a security, fractional undivided interest in oil, gas, or other mineral rights, any put, call, straddle, option, or privilege on any security, certificate of deposit, or group or index of securities (including any interest therein or based on the value thereof), or any put, call, straddle, option, or privilege entered into on a national securities exchange relating to foreign currency, or, in general, any interest or instrument commonly known as a "security", or any certificate of interest or participation in, temporary or interim certificate for, receipt for, guarantee of, or warrant or right to subscribe to or purchase, any of the foregoing." Securities Act of 1933, 15 U.S.C. § 77(b) (2012).

4 328 U.S. 293 (1946) (holding that the sale of units in a citrus grove development together with service contracts for cultivating and marketing the produce constituted a sale of securities).

Any traditional security, including an equity interest in a company,[5] a limited partner interest in a venture capital fund, and a range of other debt- and equity-like instruments, potentially can be issued as a tokenized security. In addition, tokenized securities can also be asset-backed, representing interests in real estate or fine art, among other assets. Further, the SEC and its staff (the "Staff") concluded that tokenized securities include interests in decentralized autonomous organizations.[6] Blockchain Capital is thought to have conducted the first offering of tokenized securities, also known as a security token offering ("STO"), when it raised capital for its Singapore-based fund pursuant to Regulations D and S under the Securities Act.[7]

Pursuant to Section 5 of the Securities Act, any offer or sale of a security made to U.S. persons must either be (1) registered with the SEC or (2) offered and sold pursuant to an exemption from registration. The following chart provides a summary of the unique regulatory requirements for the salient forms of offerings of tokenized securities. For more detailed information regarding each and associated legal requirements, please refer to the Appendix below.

REGISTRATION REQUIREMENTS AND RESTRICTIONS UNDER VARIOUS FORMS OF SECURITY TOKEN OFFERINGS

OFFERING TYPE	SECTION	ISSUER RQMTS	INVESTOR RQMTS	LIMITS ON AMT. RAISED	GENERAL SOLICITATION	STATE LAW PRE-EMPTION	TRANSFERS
FULL REGISTRATION	Sec. 6 Sec. Act.	None	None	None	No sales during pre-filing period	Yes, if listed on a national exchange	Freely tradeable on registered exchange or ATS
EXEMPT OFFERINGS:							
PRIVATE PLACEMENT	Sec. 4(a)(2) of Sec. Act and Reg. D (Rule 506(b) and (c))	None, but exlcudes "Bad Actors"	Accredited Investors, with "Bad Actor" exclusions Rule 506(b) permits up to 35 sophisticated but non-ac-credited investors	None	No general solicitation or advertising Rule 506(c) permits general solicitation	Section 4(a)(2) = none Reg D = yes Some reqmts to notice filings and state fees	"Restricted Securities" – not freely tradeable until expiration of restricted period; may have private transfers between accredited investors during restricted period

5 *See, e.g.*, Overstock.com's December 2015 offer of Blockchain Voting Series A Preferred Stock. https://www.sec.gov/Archives/edgar/data/1130713/000104746916016691/a2230280z424b2.htm.

6 On July 25, 2017, the SEC issued a Report of Investigation under Section 21(a) of the Securities Exchange Act of 1934 (the "Exchange Act") describing an SEC investigation of The DAO, a decentralized autonomous organization, and its offer and sale of DAO Tokens. Report of Investigation Pursuant to Section 21(a) of the Securities Exchange Act of 1934: The DAO, Exchange Act Release No. 81207 (July 25, 2017), https://www.sec.gov./litigation/investreport/34-81207.pdf ("DAO Report").The SEC applied Howey and concluded that the DAO Tokens were "securities;" see also Press Release, SEC Issues Investigative Report Concluding DAO Tokens, a Digital Asset, Were Securities (July 25, 2017), https://www.sec.gov/news/press-release/2017-131.

7 The Form D that Blockchain Capital submitted to the SEC for its Regulation D private placement is available here: https://www.sec.gov/Archives/edgar/data/1703926/000095017217000040/xslFormDX01/primary_doc.xml.

OFFERING TYPE	SECTION	ISSUER RQMTS	INVESTOR RQMTS	LIMITS ON AMT. RAISED	GENERAL SOLICITATION	STATE LAW PRE-EMPTION	TRANSFERS
EXEMPT OFFERINGS:							
PRIVATELY HELD COMPANIES	Reg. A	Privately held companies in U.S. or Canada	Tier 1 = None Tier 2 = None but non-accredited investors have investment limits	Tier 1 = $20M in 12 mo. Tier 2 = $50M in 12 mo.	None	Tier 1 = No Tier 2 = yes, pre-empted	None
CROWD-FUNDING	Reg. CF	No non-U.S., blank-check, reporting or investment cos, or "Bad Actors"	None, but investment limits based on income and net worth	$1.0M over 12 mo. period	Offered through one intermediary registered as a broker dealer or "funding portal" and also a member of FINRA	Yes	After 12 mo.

II. SECURITIES OFFERINGS WITH UTILITY TOKEN FEATURES

Tokenized securities can provide some of the benefits of a traditional security, such as a share of income or a dividend payment, or otherwise can represent an investment contract in which a purchaser acquires the tokenized security with the expectation of profits through the efforts of others. A tokenized security can also provide its holder with rights to a non-security token—either a so-called "utility token," which allows a holder to consume or redeem the token for a good or service in a functioning system, or a cryptocurrency token, which exists solely as a medium of exchange, store of value, or unit of account, like bitcoin.[8]

First, a tokenized security might represent a claim on a future, not-yet-extant non-security token (a "placeholder token"). This placeholder token will be swapped with the non-security token once the non-security token is created and the system in which the non-security token will be used is functioning and publicly available. Second, the facts and circumstances might show that the manner in which the tokenized security is used have changed such that the token no longer has the features of a security ("mutable tokens"). Third, a tokenized security might provide a dividend to its holder in the form of a second token, and that second token might constitute a non-security token ("dividend-paying tokens").

8 The SEC has repeatedly indicated that it does not view bitcoin as a security through unofficial statements. *See, e.g.*, Hearing on SEC FY19 Budget before the Fin. Serv. and Gen'l Gov't Subcomm. of the House Comm. on Appropriations, 115th Cong. (statement of Jay Clayton, Chairman, Securities and Exchange Comm'n) ("A pure medium of exchange, the one that's most often cited, is bitcoin. As a replacement for currency, that has been determined by most people to not be a security."); *see also* William Hinman, Digital Asset Transactions: When Howey Met Gary (Plastic), Remarks at the Yahoo! Finance All Markets Summit: Crypto (June 14, 2018), https://www.sec.gov/news/speech/speech-hinman-061418.

In each case, the tokenized security is designed to provide, through some mechanism, a non-security token to its holder. This section explores the legal issues surrounding these three scenarios.

The first and second types of tokenized securities described above present similar legal issues but address them in distinct ways. Currently, it is widely accepted that a pre-functionality (*i.e.*, pre-utility) sale of tokens may well constitute an "investment contract," and hence a security, within the meaning of Section 2(a)(1) of the Securities Act. This conclusion flows from the likelihood that a reasonable purchaser expects to profit in the secondary market for the tokens based on the efforts of the token seller to build the network or application in which the token is used. For example, in a 2017 Administrative Order against Munchee, Inc. (the "Munchee Order"),[9] the SEC found an investment contract based on the company "emphasiz[ing] the economic benefits to the purchaser [of a token] to be derived from the managerial efforts of the [token's] promoter." The tokens in the Munchee Order ("MUN") were intended for use in an application to advertise, review and buy meals from restaurants, although "no one was able to buy any good or service with MUN" at the time of their sale.[10] This meant that, "[a]t the time of the offering and sale of MUN tokens, no other person could make changes to the Munchee App or was working to create an 'ecosystem' to create demand for MUN tokens."[11] Thus, the SEC concluded, a purchaser of MUN was entirely reliant on the efforts of the sponsor to realize any value from his or her purchase of MUN. Given that the MUN token's value was zero when it was sold, a purchaser must have expected its value to increase due to these efforts, and a rational purchaser would only have purchased MUN in the expectation that this value increase would be great enough to constitute a profit above the purchase price. As a result, the pre-functionality MUN tokens represented an investment contract, and therefore a security.

The first and second types of the tokens discussed in this section seek to square this result with a Token Sponsor's desire to ultimately create a non-security token for general consumptive use.

TYPES OF SECURITIES TOKENS

PLACEHOLDER TOKENS

Will be swapped with a non-security token once the non-security token is created and the system in which the non-security token will be used is functioning and publicly available.

MUTABLE TOKENS

The manner in which the tokenized security is used have changed such that the token no longer has the features of a security.

DIVIDEND-PAYING TOKENS

A tokenized security might provide a dividend to its holder in the form of a second token, and that second token might constitute a non-security token.

9 Munchee Inc., Securities Act Release No. 10445 (Dec. 11, 2017), https://www.sec.gov/litigation/admin/2017/33-10445.pdf.
10 *Id.* at ¶ 10.
11 *Id.* at ¶ 33.

A. PLACEHOLDER TOKENS

Token Sponsors, as part of their token distribution may offer and sell a pre-functionality token sale agreement in accordance with Rule 506(b), Rule 506(c), or Regulation S, which represents a right, at a future time, to delivery of utility tokens. The agreement may take the form of a non-tokenized instrument, the most common of which is the Simple Agreement for Future Tokens ("SAFT"). In lieu of an agreement, a Token Sponsor might issue to purchasers a placeholder token, which would perform the same function as a SAFT or other non-token contract or instrument. In either case, the pre-functionality instrument is a security, and it is subject to the registration and exemption provisions of the Securities Act. At the point at which the future non-security tokens achieve a sufficient level of functionality, such that their value derives from the value of the services provided on and through the platform and not on the efforts of the persons who organized the enterprise to build out the platform, the pre-functionality security is effectively extinguished and the holder thereof receives delivery of the tokens; if the instrument is itself tokenized (i.e., placeholder token), then the token sponsor most often will effect an exchange between the placeholder token and the functional non-security token and will destroy, or "burn," the placeholder tokens.[12]

A pre-functionality token that promises the delivery of a specified amount of a future token at a specified price on a future date has many of the characteristics of a forward contract for the underlying future tokens. It is established that a forward or futures contract for non-securities, in fact any type of sales contract, normally does not entail an investment contract. For example, in SEC v. Commodity Options International, Inc., the Ninth Circuit stated that:

> ***Commodity futures contracts are considered not to be securities per se. They are investments to be sure. The investment, however, is not in an enterprise but is in the underlying commodity, and we may assume, arguendo, that a conventional option to buy or sell a futures contract takes on the character of the contract that is the subject of the option and is no more a security than is that underlying contract.***[13]

A pre-functionality token differs from conventional forward contracts in an important respect: it typically involves a to-be-created novel product or service with no established market or value. In the words of the Ninth Circuit, such instruments are often "investments in the enterprise" of creating an operating token rather than an investment in just the token.

This would be the case if development of the functionality of the relevant platform allowed tokens to be used for their intended purpose on that platform at the time of the token swap. So long as there are no other efforts of others involved either—*i.e.*, (i) marketing materials are focused primarily on present functionality and use of the token, (ii) the seller has not built features into the token intended

12 *See* Larry E. Bergmann, Updating SAFT: Breaking the Security/Utility Token Conundrum, Blockchain Law Center (June 12, 2018), https://www.blockchainlawcenter.com/newsitem/news/updating-saft-breaking-the-security-utility-token-conundrum-543/.

13 553 F.2d 628, 632 (9th Cir. 1977) (internal citations omitted).

to provide an investment return or support the price of the token in secondary markets, and (iii) the seller does not promise to take steps to support secondary trading of the token—then, at this stage, the seller's efforts would be limited to supporting the use of the tokens with the network or software application and any further increase in the value of the token should be derived from the efforts of others. Once the post-functionality tokens are delivered to the purchasers, each purchaser would have unfettered control over the tokens, and would have no reasonable expectation that the seller will take future steps intended to increase the market value of the tokens. Generally, "the courts will find a security is not present where the investor retains unfettered discretion over the distribution and marketing of the product."[14] At this point, unlike the DAO Token, which promised returns from projects undertaken by the DAO, any reasonable expectation of profits the purchaser might have should depend primarily on the market's demand for the functioning application and the purchaser's own efforts to find buyers and negotiate a favorable price for the tokens (akin to general expectations of appreciation in the demand for a commodity or real estate).

B. MUTABLE TOKENS

> **"CAN A DIGITAL ASSET THAT WAS ORIGINALLY OFFERED IN A SECURITIES OFFERING EVER BE LATER SOLD IN A MANNER THAT DOES NOT CONSTITUTE AN OFFERING OF A SECURITY?"…"CASES WHERE . . . THE DIGITAL ASSET IS SOLD ONLY TO BE USED TO PURCHASE A GOOD OR SERVICE AVAILABLE THROUGH THE NETWORK ON WHICH IT WAS CREATED[,] I BELIEVE IN THESE CASES THE ANSWER IS A QUALIFIED 'YES.'"**
>
> *— **William Hinman**, Director of the Division of Corporate Finance at the Securities and Exchange Commission, June 2018.*

Rather than issue a placeholder token that later is swapped for a post-functionality utility token, a Token Sponsor might choose to sell a pre-functionality token as a security, then subsequently develop the system in which the token ultimately will operate and, upon deploying the system, allow token holders to utilize that same token within the system and enjoy its consumptive value. Critical, and unique to tokens and this analysis, is the mutability of the token—it can be both initially representative of an investment opportunity and subsequently a functional tool for use on the blockchain application. As William Hinman, Director of the Division of Corporate Finance at the Securities and Exchange Commission, noted in remarks in June 2018: "the analysis of whether something is a security is not static and does not strictly inhere to the instrument."[15] Rather, when asking "Can a digital asset that was originally offered in a securities offering ever be later sold in a manner that does not constitute an

14 Wabash Valley Power Ass'n, Inc. v. Public Serv. Co. of Ind., Inc., 678 F. Supp. 757, 767 (1988).
15 Hinman *supra* note 8.

offering of a security?," Hinman asserted that, in "cases where . . . the digital asset is sold only to be used to purchase a good or service available through the network on which it was created[,] I believe in these cases the answer is a qualified 'yes.'"[16] By rendering the facts and circumstances surrounding the token such that it has functionality, the Token Sponsor may effect the evolution and development of the token from a pre-functionality security to a post-functionality non-security. Thus, rather than swapping one token for another, the token sponsor allows the single token to evolve from a security to a non-security. An investment contract arises from the understanding as to how the token will be developed into something of useful value; as that development occurs, those features that suggest that a token represents a security may fade in relevance or otherwise disappear and be replaced by features that suggest that the token represents a consumptive utility token or other non-security.

Such changing circumstances – achieving the functionality of the token – also allow the seller to take a different approach to marketing its network or software application, further modifying the extant facts and circumstances surrounding the token. The completion of the network or software application such that the tokens are immediately usable for their intended purpose allows the seller to focus on potential users, so any marketing materials would emphasize the value in using the goods and services accessible through the token. If the tokens are not digital securities by design, and if all the other facts and circumstances support the conclusion that the tokens sold at the time of the token sale should no longer be viewed as investment contracts, then tokens received by pre-functionality purchasers under those same circumstances should not be viewed as investment contracts either. The characteristics of the pre-functionality token sale by which the tokens were originally purchased should not be determinative of the status of the tokens as "investment contracts" with respect to the subsequent status of the tokens under changed facts and circumstances. Indeed, as CFTC Commissioner Brian Quintenz has recognized, that virtual currencies "can transform. They may start their life as a security from a capital-raising perspective but then at some point – maybe possibly quickly or even immediately – turn into a commodity."[17]

C. DIVIDEND-PAYING TOKENS

The third situation involving a security token that produces a non-security token for its holder is the most straightforward: a security token that delivers a dividend payment, either a pro rata share of income or otherwise, to its holder in the form of a second, distinct, non-security token. It is difficult to envision a situation where the dividend-paying token would not represent a security, because a reasonable purchaser would only acquire it to enjoy the passive income derived from the efforts of others. The token received as a dividend, however, need not necessarily be a security. If the dividend token were either a pure cryptocurrency, like bitcoin, with value only as a medium of exchange, store of value, or unit of account, then, like bitcoin, it would be less likely to be viewed

16 *Id.*
17 Matthew Leising and Brian Louis, Industry Executives Think a Bitcoin ETF Is on Its Way, Bloomberg (Oct. 19, 2017), https://www.bloomberg.com/news/articles/2017-10-19/a-bitcoin-etf-may-be-the-next-big-thing-on-u-s-exchanges.

as itself a security. Alternatively, if the dividend token were a post-functionality utility token, which could be used for some consumptive purpose in an existing system, then it might fall outside of the definition of a security. The best way to think about this is to change one fact from the *Howey* case itself – suppose the purchasers of interests in the citrus grove were paid in oranges instead of cash. If all the other facts remained the same, we would undoubtedly still consider the contracts representing the interests to be an investment contract (it would still be a contract to share profits, just denominated in oranges), but we would never conclude that the oranges, once fully grown and delivered, had somehow transformed into a security that could not be immediately sold by the purchasers upon receipt.

It is worth noting two scenarios that, on their face, might appear comparable to the dividend-paying token system but that differ in material ways from the dividend-paying token scenario. The differing facts and circumstances allow for an argument that neither token is a security. While these scenarios fall outside of the scope of this paper, it is worth briefly making note of each. First, a blockchain that uses a proof-of-stake consensus mechanism[18] might require a user to stake one token and receive a different token as his or her staking reward. In this case, the user is not receiving passive income through the efforts of others, but rather is receiving a reward for his or her own efforts—namely, providing computing power to assist with the maintenance of the blockchain. Accordingly, in this case, both the staking token and the reward token might not represent investment contracts under the *Howey* test. Second, a system involving a so-called "stablecoin" – a token for which the value is pegged to an external value, such as fiat currency, cryptocurrency, or other financial asset, or an algorithm, designed to limit price volatility. Users would hold the minting token and, by virtue of holding it, receive a variable number of stablecoins on a regular basis, with the number of stablecoins received governed by the system's algorithmic assessment of the change in supply necessary to maintain price stability. In this case, a suitably decentralized system might render the efforts of others irrelevant to the minting token's value.

STABLECOIN

A token for which the value is pegged to an external value, such as fiat currency, cryptocurrency, or other financial asset, or an algorithm, designed to limit price volatility

In both scenarios, the facts and circumstances specific to a given token will be key, and it is entirely possible that, in many variations of these scenarios, the staking token or the minting token would represent a security. Because one can envision scenarios where that might not be the case, however,

18 *See* Proof of Stake FAQs, GitHub, https://github.com/ethereum/wiki/wiki/Proof-of-Stake-FAQs (last visited Apr. 25, 2019).

these two scenarios should be considered distinct from the dividend-paying token discussed above, which in every case would presumably represent a security.

III. U.S. REGULATION OF OVERSEAS TOKEN OFFERINGS

U.S. and foreign companies seeking to conduct a token offering outside the United States should be mindful of the broad application of U.S. federal securities laws. The token sold in a non-U.S. token offering might not be a security under the laws of that jurisdiction, but that same token might be viewed as security under the securities laws of the United States. In light of the potential application of U.S. securities laws to offshore offerings, a company should consider whether its token offering and resales of those tokens should either be registered under the Securities Act of 1933[19] (the "Securities Act") or comply with an exemption from registration under Section 5 of the Securities Act.[20]

Exemptions from SEC registration that an issuer may rely upon include Regulation D[21] and Regulation S.[22] Regulation S provides a non-exclusive safe harbor for extraterritorial offers, sales, and resales of securities in Rules 903 (safe harbor for issuers and "distributors"[23] of securities and their respective affiliates) and 904 (resale safe harbor) under the Securities Act.[24] While transactions falling outside of the Regulation S safe harbor might still be deemed to occur outside of the United States if there is an insufficient nexus to the United States,[25] compliance with Regulation S provides certainty. In the context of a global offering, the non-U.S. Regulation S offering is often conducted with a concurrent Regulation D private placement to accredited investors in the U.S. Regulation S, however, does not exempt a transaction from the antifraud provisions of U.S. securities laws.

Demonstrating compliance in the context of an initial sale may include obtaining appropriate representations from the buyer, and if an offer is conducted online, the implementation of "geofencing" of websites or similar restrictions. It is important to take such precautions in order to ensure that a sale is being marketed and is intended solely as an offshore transaction.

A. CATEGORIZATION OF TRANSACTIONS UNDER REGULATION S

The safe harbor provided by Regulation S contains three categories of offerings for an offer or sale by an issuer, "distributor", or affiliates or persons acting on their behalf, depending on whether the issuer

19 15 U.S.C § 77a *et seq.*
20 15 U.S.C § 77e.
21 17 C.F.R. § 230.500 *et seq.*
22 17 C.F.R. § 230.901 *et seq.*
23 "Distributor" means any underwriter, dealer, or other person who participates, pursuant to a contractual arrangement, in the distribution of the securities offered or sold in reliance on Regulation S. 17 C.F.R. § 230.902(d).
24 17 C.F.R. § 230.903; 17 C.F.R. § 230.904.
25 There has long been a longstanding recognition that if legislative text of a U.S. law does not speak of extraterritorial application, then there is a presumption against extraterritorial application of such U.S. law. *See* Foley Bros Inc v Filardo, 336 US 281, 285 (1949); Equal Employment Opportunity Commission v Arabian American Oil Co, 499 US 244, 248 (1991). In 2010, the Supreme Court held in Morrison V. National Australia Bank that the anti-fraud provisions in Section 10(b) of the Exchange Act do not provide a right to sue in transactions taking place outside the U.S. *See* 561 US 247 (2010). The Court held that Section 10(b) only reaches "transactions in securities on domestic exchanges, and domestic transactions in other securities." As a result, many have taken the view that the Court's reasoning applies to the U.S. securities laws generally unless Congress has affirmatively called for offshore application of such laws in a statute. However, Congress has subsequently amended the Securities Act and the Exchange Act to provide that the SEC may exercise jurisdiction over offshore transactions in its enforcement actions in certain circumstances.

is (i) foreign or domestic, (ii) issuing debt or equity securities and (iii) a reporting company under the Exchange Act,[26] as well as the nature of the transaction itself. The levels of procedural safeguards vary with the three categories. For purposes of determining what category a transaction falls into and what restrictions apply, three threshold questions must be answered:

HOW TO DETERMINE THE CATEGORIZATION OF A TOKEN UNDER REGULATION S

1	2	3
IS THE TOKEN DEBT OR EQUITY?	IS THE ISSUER "FOREIGN" OR "DOMESTIC"?	IS THE ISSUER A REPORTING COMPANY UNDER THE EXCHANGE ACT?

Is the Token Debt or Equity? Regulation S requires a security to be classified either as debt or as equity.[27] However, digital tokens often have more complex hybrid features than traditional debt or equity securities and may not fit neatly within either category. Unless a token has clear hallmarks of a debt security,[28] a more conservative approach would be to classify most tokens as equity securities for purposes of the safe harbor.

Is the issuer "foreign" or "domestic"? Greater restrictions generally apply to "foreign" issuers than "domestic" issuers. A "foreign issuer" is a "foreign government" or "foreign private issuer."[29] The determination of foreign private issuer status is highly technical. A foreign incorporated entity will not be a foreign private issuer if more than 50% of its outstanding voting securities are held by U.S. residents and any one of the foregoing applies: (i) the majority of its executive officers or directors are U.S. citizens or residents, (ii) more than 50% of the issuer's assets are located in the United States, or (iii) the issuer's business is administered principally in the United States.[30] A "domestic issuer" is in turn any issuer other than a foreign private issuer or foreign government.[31]

Is the issuer a reporting company under the Exchange Act? Currently, few issuers of digital tokens would be registered as reporting issuers with the SEC under the Exchange Act, but that may change in the future.

26 15 U.S.C § 78a *et seq.*
27 The term "equity security" is defined to mean any stock or similar security, certificate of interest or participation in any profit sharing agreement, preorganization certificate or subscription, transferable share, voting trust certificate or certificate of deposit for an equity security, limited partnership interest, interest in a joint venture, or certificate of interest in a business trust; any security future on any such security; or any convertible security, warrant or any right, put, call, straddle, or other option or privilege of buying such a security from or selling such a security to another without being bound to do so. *See* 17 C.F.R. § 230.405.
28 Debt securities of an issuer is defined to mean any security other than an equity security as defined in 17 C.F.R. § 230.405, as well as the following: (1) Non-participatory preferred stock; and (2) certain asset-backed securities.
29 *See* 17 C.F.R. § 230.902(e).
30 *See* 17 C.F.R. § 240.3b-4(c).
31 *See* 17 C.F.R. § 230.902(e).

B. IMPLEMENTATION OF RESALE RESTRICTIONS ON SECURITY TOKENS

Traditional means of implementing required restrictions on the resale of securities include issuing physical certificates, legending securities and offering materials, requiring purchaser or transferee certifications and legal opinions for transfer, and issuing stop transfer instructions for the issuer of securities. These measures can be effective for traditional securities but are often inefficient and overly restrict compliant resale transactions. Security tokens in turn present unique challenges for demonstrating compliance with applicable restrictions in light of the absence of physical certificates for securities, the absence of a central transfer agent to record transactions and act as a gatekeeper for transactions, the global distributed nature of participants and the liquidity provided by global trading platforms. Smart contracts and blockchain technology platforms are starting to come online to offer better ways to police restrictions and facilitate compliant resales of securities for the issuer of securities.

Below are some examples of such restriction methods that would naturally be applied to STOs.

- **Restrictive Legends.** Legends advising on the resale restrictions can be included on the relevant token sale documentation, including the token white paper, token sale terms, and purchase agreements. As discussed further below, restrictive legends can also be written into smart contracts associated with the token to ensure that resale restrictions are included on future transfers. The SEC has indicated that adding precautionary legends on securities requiring the purchasers to represent that they are not acquiring the securities for distribution, and in the case of equity securities, issuing stop-transfer instructions to the transfer agent prohibiting the transfer of the security, can be effective means of preventing illegal distributions. However, these methods are not regarded as a basis for an exemption from registration. The nature of the purchaser's past investment and trading practices or the character and scope of the purchaser's business may indicate an intent to resell securities despite representations obtained through legending.

- **Legal Opinion Requirements.** Requiring the seller of a token to provide a legal opinion to the issuer that resale is permitted is an expensive approach that can limit otherwise compliant transactions but may be appropriate for circumstances that do not fit within a clear safe harbor.

- **Repurchase Rights.** Requiring token purchasers to agree to the issuer's rights to repurchase the tokens if transfer restrictions are not complied with can also provide the issuer with a method to address noncompliant transfers.

- **Multi-Signature Wallets.** Multi signature wallets requiring more than one signature to authorize a transaction can be used to limit token transfers to approved purchasers.

- **Smart Contract Restrictions.** This method involves writing transfer terms and restrictions into the token smart contract. For example, the smart contract can be written to limit transfers of the token to certain categories of purchasers or purchasers who meet the requirements of a resale

exemption by adding a validation requirement in the smart contract's code. These restrictions can be customized to prohibit all token transfers, to allow transfers to receivers who meet certain requirements and/or to have token transfer restrictions fall away after a specified period of time. If the Regulation S exemption is used, transfers can be limited to whitelisted Non-US buyers located outside of the U.S. In the alternative, another option would be to condition any transfer upon the consent of the issuer so that the issuer can take steps to ensure that future transfers are made in compliance with a valid resale exemption.

- **Contractual Lock-Ups.** Token purchasers can be required to enter into lock-up provisions limiting the purchaser's ability to resell tokens in order to comply with requirements for a resale exemption. For example, to comply with the distribution compliance periods required by Regulation S, lock up periods can be added for each token purchaser, either in a traditional contract or written into smart contract code. Not all securities traded in compliance with Regulation S requirements subsequently become freely tradable, but addressing a lock up period in a smart contract can also allow tokens that are not equity securities issued by a domestic issuer to become freely tradable as soon as the required holding period is reached.

C. OFFSHORE RESALES OF SECURITIES

A person who bought a restricted security in a securities token offering would have to resell the securities under an exemption from U.S. securities laws. Section 4(a)(1) of the Securities Act generally exempts resales of restricted securities by a person who is not an issuer, underwriter or dealer. The holder of restricted securities would need to demonstrate that he or she did not purchase the securities with a view towards reselling it because of the expansive definition of "underwriter" under U.S. securities laws. The purchase could also resell under applicable safe harbors, which typically would require the purchaser to hold the securities for a specified period. Available and relevant provisions include Rule 144 (non-exclusive safe harbor from statutory underwriter status) and Rule 904 of Reg S (safe harbor for the resale of securities by a person other than the issuer).

An STO offered to non-US persons can effectively be structured with legal advice customized to the facts and circumstances of a particular issuer and leveraging available technology to yield a compliance process which is not overly restrictive.

D. OTHER GLOBAL TRADING CONSIDERATIONS

Additional trading considerations also arise from the differing approaches taken by jurisdictions other than the United States in regulating digital tokens. For example, a holder of a digital token issued in a jurisdiction where it would be classified as something other than a security) may seek to sell the token to U.S. persons. When viewed from a U.S. securities law perspective, the digital token could be viewed as a security token, which would make such sale subject to the trading restrictions and requirements under Regulation S. Issuers who are conducting utility token offerings outside of the United States

should therefore be cognizant of the issuance and resale restrictions under Regulation S, particularly if there is a possibility of such tokens being traded into the United States or to U.S. persons.

E. APPLICABILITY OF BLUE SKY LAWS

In addition to the federal securities laws, state securities or blue sky laws apply to the offer and sale of securities. Unless federal preemption of state law applies, offers and sales of securities in different states need to be registered or qualified in those states or fall within an available exemption. Because registration or qualification in 50 states can be burdensome and time-consuming, issuers of traditional securities seek to rely on federal preemption or limit the offering to fit within state law restrictions where applicable.

The National Securities Markets Improvements Act of 1996, as amended (the "NSMIA")[32] preempts the registration requirement of state blue sky laws from applying to certain "covered securities."

In addition to federal preemption, states have a variety of exemptions that are potentially applicable to certain facts and circumstances and can vary considerable from state to state. Some states have exemptions for exchange-listed issuers, which could be useful if an issuer with a class of securities already listed on an exchange (the list of eligible exchanges varies from state to state) wanted to issue tokens, since other securities of listed issuers may be exempt under these provisions. In addition, many states have exemptions for certain "blue chip" issuers, issuers who are listed in certain manuals (so-called "manual listings"), as well as for securities registered under the Securities Act, exemptions for limited offerings, or to various exemptions for transactions involving sophisticated investors.

If a token or transaction is not preempted or exempted from blue sky law, then a full blue sky registration process must be undertaken which, depending on the states involved, can be very difficult and time consuming. Methods of registration vary from state to state, but most states have adopted one or more of registration by: notification, coordination and qualification. Certain eligible issuers may also qualify for registration by qualification whereby designated states can take the lead in the review process on behalf of certain other states.

One key distinction of the blue sky review process when compared to the federal review process for a registered offering is that the federal review process only involves review of disclosure, while the states will actually evaluate the merit of an offering, including the terms of a security to evaluate whether a transaction is unfair to prospective purchasers or subjects them to unreasonable risks. If a state regulator is not satisfied as to the merits of an offering, it can stop the offering from taking place within the state. Tokenized securities may be subject to heightened scrutiny compared with traditional securities.

32 Pub. L. No. 104-290, 110 Stat. 3416 (codified in various sections of the Securities Act, in particular Section 18 of the Securities Act).

IV. TRADING TOKENIZED SECURITIES

Purchasers of tokenized securities need liquidity for the securities that they buy in such issuances. The development of secondary markets is therefore crucial to the growth of tokenized security issuance. The following sections address legal and regulatory considerations relating to secondary markets for tokenized securities.

A. TRADING PLATFORMS

As a general rule, securities trade on one of two types of regulated markets: registered national securities exchanges and alternative trading systems ("ATSs"). Registered national securities exchanges and ATSs, while operating in similar manners, are subject to separate regulatory regimes and registration requirements. The NYSE and NASDAQ are examples of NSEs. A tZERO subsidiary offers an ATS, allowing tZERO tokenized securities to be traded.

A national securities exchange must register with the SEC under the Exchange Act through an application process.[33] The SEC must also find that the national securities exchange has rules that meet certain criteria.[34]

An ATS, unlike a national securities exchange, does not have to obtain SEC approval before commencing operations. Rather, to become an ATS, Rule 301(b) of Regulation ATS requires an entity to register as a broker-dealer and to file Form ATS with the SEC. Broker-dealer registration broadly consists of two components. First, the ATS must file Form BD with the SEC.[35] Form ATS is not an application and the SEC does not "approve" an alternative trading system before it begins to operate. However, the SEC staff will often undertake an informal review of a Form ATS and provide comments, and the ATS will need to address any deficiencies noted by the SEC staff during this informal review. Failure to do so before beginning operations could result in a referral to enforcement for having a deficient Form ATS. Second, a broker-dealer must become a member of a self-regulatory organization ("SRO"),[36] typically FINRA.[37]

1. MEMBERSHIP

Section 6(c)(1) of the Exchange Act prohibits exchanges from granting membership to any person not registered as a broker-dealer or associated with a broker-dealer.[38] Consequently, non-broker-dealer institutions cannot be members of a national securities exchange. However,

33 15 U.S.C § 78f.
34 *See* 15 U.S.C. § 78f(b)(1). *See generally* 15 U.S.C. § 78f(b)(2) through (10).
35 17 C.F.R. § 242.301(b). Within 45 days of filing a completed Form BD, the SEC will either grant registration or begin proceedings to determine whether it should deny registration. Typically, the SEC grants registration of a broker-dealer on Form BD within a few days if the form has been properly completed.
36 Section 3(a)(26) of the Exchange Act defines "self-regulatory organization" as "any national securities exchange, registered securities association, or registered clearing agency, or (solely for purposes of sections 19(b), 19(c), and 23(b) of this title) the Municipal Securities Rulemaking Board established by section 15B of this title."
37 Unless a broker-dealer limits its security transactions solely to a national securities exchange of which it is a member, Section 15(b)(8) of the Exchange Act and Rule 15b9-1 thereunder require the broker-dealer to become a member of FINRA.
38 15 U.S.C. § 78f(c)(1).

ATSs are not subject to a similar restriction; therefore, an ATS can have non-broker-dealer institutional subscribers that directly access the ATS.[39]

2. DISCLOSURE OF OPERATIONS

National securities exchanges are subject to comprehensive rule filing requirements under Section 19(b) of the Exchange Act, requiring both their trading rules as well as details regarding their trading operations to be made public.[40] Any time a national securities exchange seeks to change its rules, it must first file a rule amendment with the SEC on Form 19b-4, which, if non-controversial, can become immediately effective upon filing, or otherwise be subject to public comment before SEC approval.

In contrast, an ATS has limited disclosure requirements, even to the SEC.[41] Form ATS is deemed confidential when filed. As a result, unless voluntarily provided to the public, the Form ATS is generally not available even to subscribers to the ATS. Additionally, only material changes must be filed with the SEC before implementation;[42] all other changes need to be filed on an amended Form ATS within 30 days after the end of each calendar quarter.[43]

3. LISTING OF SECURITIES

Section 12 of the Exchange Act prohibits a security from trading on a national securities exchange unless there is an effective registration with respect to such security for the exchange.[44] Once a security is registered and listed on an exchange, other exchanges may extend unlisted trading privileges to the security pursuant to Section 12(f) of the Exchange Act.[45]

An ATS must satisfy a similar gating function with respect to securities traded on the ATS. In particular, a broker-dealer wishing to publish any quotation for a security in a "quotation medium" (which includes an ATS) to gather specified information regarding the issuer.[46] Once a broker satisfies these information-gathering requirements and has begun quoting in the subject security, other brokers can "piggyback" on such quotations without having to satisfy the requirements.[47]

39 17 C.F.R. § 242.300, 301.
40 15 U.S.C. § 78o.
41 The SEC has proposed rules to expand the disclosure requirements for ATSs trading an "NMS Stock," which includes any security or class of securities (other than an option) for which transaction reports are collected, processed, and made available pursuant to an effective transaction reporting plan, other than a listed option. See Securities Exchange Act Release No. 76474 (Nov. 18, 2015). A security that is traded solely in the over-the-counter market is unlikely to fall within this definition. To date, the SEC has not taken further action on this proposal.
42 17 C.F.R. § 242.301(b)(2)(ii).
43 17 C.F.R. § 242.301(b)(2)(iii).
44 15 U.S.C. § 78l.
45 15 U.S.C. § 78l(f).
46 17 C.F.R. § 240.15c2-11.
47 17 C.F.R. § 240.15c2-11(f)(3).

4. DISPLAY OF QUOTATIONS

The SEC mandates in Regulation NMS that all national securities exchanges make available the best bid, the best offer, and aggregate quotation sizes for each security traded on that exchange.[48] Further, the SEC directs that all national securities exchanges act together to develop a national market system plan for the collection and consolidation of such quotation information into a single quotation stream.[49]

Unlike a national securities exchange, an ATS only has to display its quotations for inclusion in the public quote stream under specified circumstances. First, and most importantly, an ATS is only required to make its quotations available with respect to NMS stocks.[50] As a result, unless the security on the ATS is also being traded on a national securities exchange, it is unlikely that the ATS would ever have to provide its quotations in such a security to the public quote stream. Additionally, even if the security is an NMS stock, trading volume on the ATS would have to cross certain thresholds (five percent or more of the average daily trading volume) with respect to such security for at least four of the preceding six months before the ATS would be required to disseminate its quotation information in the public quote stream.[51]

Finally, an ATS could decide to remain completely dark (not display its quotations to any person other than an employee of the ATS) and thus not subject to publishing its quotations in the public quote stream.[52]

5. FINRA AND SEC RULES APPLICABLE TO ATS AND BROKER-DEALERS

As a broker-dealer, an ATS also will be subject to the full panoply of FINRA and SEC rules and regulations applicable to broker-dealers generally. For example, as a broker-dealer, an ATS would be subject to securities transaction reporting and broker-dealer net capital and books and records requirements, among others. Finally, Regulation SCI applies a set of rigorous cybersecurity requirements both to self-regulatory organizations, such as exchanges, and to certain ATSs.[53]

48 17 C.F.R. § 242.602.

49 17 C.F.R. § 242.603. It is the combination of these two mandates that results in the creation of the Securities Information Processors ("SIPS") and dissemination of best bids and best offers (and respective sizes) from all exchanges in the public quote stream. All national securities exchanges provide quotation information and last sale information to the SIPs for the national market system plans governing trading in NYSE listed securities ("Tape A securities"), NASDAQ listed securities ("Tape C securities"), and securities listed on exchanges other than NYSE or NASDAQ ("Tape B securities"). The SIPs consolidate this information and disseminate the consolidated information to market participants.

50 17 C.F.R. § 242.301(b)(3)(i). Rule 300(g) of Regulation ATS provides that that neither a debt security nor a convertible debt security is an NMS stock for purposes of Regulation ATS. 17 C.F.R. § 242.300(g). We do not think that, at least initially, the securities that will trade on the Platform will be NMS securities because they are not likely to be securities for which transaction reports are collected, processed, and made available pursuant to an effective transaction reporting plan.

51 17 C.F.R. § 242.301(b)(3)(i)(B).

52 17 C.F.R. § 242.301(b)(3)(i)(A).

53 17 C.F.R. § 242.1000 *et seq.* (2017).

B. TRANSACTION PROCESSING

After a transaction is effected on a market, the securities and associated payment must be processed and transferred between the parties. This activity raises potential issues with respect to "clearing agency" and "transfer agent" regulation.

CLEARING AGENCY

Acts as an intermediary in making payments or deliveries or both in connection with transactions in securities; or otherwise permits or facilitates the settlement of securities without physical delivery of securities certificates.

TRANSFER AGENT

Person who engages on behalf of an issuer or on behalf of itself as an issuer in:

1. registering the transfer of securities; or
2. transferring record ownership of securities by bookkeeping entry without physical issuance of securities certificates.

BROKER - DEALER

Obtains custody of its customers' securities by maintaining "physical possession or control of all fully paid securities and excess margin securities carried by a broker or dealer for the account of customers."

1. CLEARING AGENCY

A "clearing agency," among other things, "acts as an intermediary in making payments or deliveries or both in connection with transactions in securities;" or

Otherwise permits or facilitates the settlement of securities without physical delivery of securities certificates.[54]

If the trading platform, in addition to executing transactions between the parties to a trade, also performs a function described above in effecting the transfer of securities and payments between transaction parties, then the platform may be performing the functions of a clearing agency. A clearing agency must register with the SEC, a lengthy process.[55] Clearing agency concerns may arise if, for example, a trading platform maintains wallets for its subscribers/members and securities and cash (cryptocurrencies or fiat currency) traded on the platform move between those wallets. The question is whether the platform's role in the movement of assets between traders constitutes a clearing agency function. The SEC has issued a warning that the need for clearing agency registration should be evaluated.[56]

54 15 U.S.C. § 78c(a)(23)(A).

55 15 U.S.C. § 78q-1(b)(2); *see* Exchange Act Sections 17A(b)(2) and 19(a), 15 U.S.C. §§ 78q-1(b)(2), 78s(a), and Rule 17Ab2-1 thereunder, 17 C.F.R. § 240.17Ab2-1.

56 "[S]ome platforms offer digital wallet services (to hold or store digital assets) or transact in digital assets that are securities. These and other services offered by platforms may trigger other registration requirements under the federal securities laws, including broker-dealer, transfer agent, or clearing agency registration, among other things." Statement on Potentially Unlawful Online Platforms for Trading Digital Assets, Sec. and Exch. Comm'n (Mar. 7, 2018), https://www.sec.gov/news/public-statement/enforcement-tm-statement-potentially-unlawful-online-platforms-trading.

There may be exceptions to registering a trading platform as a clearing agency. For example, broker-dealers registered with the SEC that are engaged in activities that fall within the definition of clearing agency are excepted from also registering with the SEC as such if the activities constitute customary brokerage activities.[57]

2. TRANSFER AGENT

A "transfer agent" is defined in Exchange Act Section 3(a)(25) and includes a person who engages on behalf of an issuer or on behalf of itself as an issuer in:

1. registering the transfer of securities; or
2. transferring record ownership of securities by bookkeeping entry without physical issuance of securities certificates.[58]

A person that performs this function (or other defined functions) must register with its "appropriate regulatory agency"[59] as a transfer agent pursuant to Exchange Act Section 17A(c) if it is performing such functions for certain securities.[60] Although it may appear to be a relatively obscure recordkeeping operation, the SEC has emphasized the important function that transfer agents perform.[61]

Prospective issuers of digital securities may consider making offerings pursuant to SEC Regulation A.[62] An issuer that has issued securities pursuant to Tier 2 of Regulation A[63] and is required to file reports pursuant to Rule 257(b) of that regulation,[64] is not required to include such securities as "held of record" if, inter alia, it satisfies the conditions of Securities Act Rule 12g5-1((b)(7).[65] One of the conditions of this exemption is that the issuer must engage a registered transfer agent with respect to such securities.[66] One effect of this provision is that an issuer that has issued securities only pursuant to Tier 2 of Regulation A is not required to register its securities under Section 12, but, as noted, must utilize a registered transfer agent.

57 *See* Exchange Act Section 3(a)(23)(B), 15 U.S.C. § 78c(a)(23)(B). That subsection also excludes certain banks engaged in customary banking activities from the definition of "clearing agency."
58 15 U.S.C. § 78c(a)(25)(C) and (E).
59 *See* Exchange Act Section 3(a)(34); 15 U.S.C § 78c(a)(34).
60 15 U.S.C. § 17q-1(c). *See also* Exchange Act Rule 17Ac2-1. *See generally* SEC, Division of Trading and Markets, "Transfer Agents," https://www.sec.gov/divisions/marketreg/mrtransfer.shtml.
61 "As agents for issuers, transfer agents play a critical role with respect to securities settlement, though they rarely receive much public attention." Securities Exchange Act Release No. 76743 (December 22, 2015), 80 Fed. Reg. 81848, 81949, https://www.gpo.gov/fdsys/pkg/FR-2015-12-31/pdf/2015-32755.pdf (proposing extensive changes to transfer agent regulation).
62 17 C.F.R. § 230.251-263. *See* Larry E. Bergmann, Regulation A as a Financing Alternative for Securities "Tokens": Some Considerations, Blockchain Law Center (Mar. 14, 2018), https://www.blockchainlawcenter.com/newsitem/news/regulation-a-as-a-financing-alternative-for-securities-tokens-some-considerations/.
63 Securities Act Rule 251(a)(2); 17 C.F.R. § 230.251(a)(2).
64 17 C.F.R. § 230.257(b).
65 17 C.F.R. § 230.12g5-1(b)(7).
66 Rule 12g5-1(b)(7)(iii), 17 C.F.R. § 230.12g5-1(b)(7)(iii).

C. CUSTODY – BROKER-DEALERS

A broker-dealer's obligation to "custody" the securities it carries for its customers is set out in Rule 15c3-3 under the Exchange Act. In particular, a broker-dealer obtains custody of its customers' securities by maintaining "physical possession or control of all fully paid securities and excess margin securities carried by a broker or dealer for the account of customers."[67] Control means that the broker-dealer holds the securities in one or more locations specified in Rule 15c3-3(c) "and free of any liens or any interest that could be exercised by a third party to secure an obligation of the broker-dealer."[68] Neither the SEC nor its staff has issued guidance on how a broker-dealer must comply with Rule 15c3-3 in obtaining custody of tokenized securities.[69]

1. POSSESSION OF TOKENIZED SECURITIES

A broker-dealer arguably could maintain the equivalent of physical possession, as that term is used in paragraph (b) of Rule 15c3-3, of customers' tokenized securities by holding those securities in wallets that the broker-dealer maintains for customers and for which the broker-dealer maintains the private keys. An auditor could confirm the broker-dealer's wallet holdings by requiring the broker-dealer to send messages from the wallets. The broker-dealer would carry customer tokenized securities long in customers' accounts, and the securities holdings in those accounts could be reconciled with the holdings in wallets maintained for the customers. This approach would be similar to the manner in which broker-dealers maintained physical possession of certificated securities. Broker-dealers often held customers' securities certificates in vaults and carried those positions long in customers' accounts. In this case, wallets and private keys would serve the same function as vaults.

2. CONTROL OF DIGITAL SECURITIES

Tokenized securities are not expected to be held at any of the control locations specified in paragraph (c) of Rule 15c3-3. Of the control locations enumerated in paragraph (c), only a securities depository, such as The Depository Trust Company ("DTC"), or a bank could hold tokenized securities. Moreover, the term "bank," as used in Rule 15c3-3, primarily includes federally-supervised banks. To date, federal bank agencies have not permitted federally-chartered banks to hold tokenized securities.

Paragraph (c)(7) of Rule 15c3-3 permits the SEC to designate (on a case-by-case basis) additional good control locations for purposes of complying with Rule 15c3-3. The staff of the SEC's Division of Trading and Markets (the "Staff") has issued guidance on "good" control

67 17 C.F.R. § 240.15c3-3(b)(1).
68 Financial Responsibility Rules for Broker-Dealers, Release No. 34-70072, 78 Fed. Reg. 51,824 (Aug. 21, 2013), https://www.govinfo.gov/content/pkg/FR-2013-08-21/pdf/2013-18734.pdf.
69 Note, however, that the SEC Division of Trading and Markets and the FINRA Office of General Counsel issued Guidance describing regulatory gray areas. Joint Staff Statement on Broker-Dealer Custody of Digital Asset Securities, SEC (July 8, 2019), https://www.sec.gov/news/public-statement/joint-staff-statement-broker-dealer-custody-digital-asset-securities.

locations for "traditional" uncertificated securities.[70]

A broker-dealer arguably could rely on transfer agents as good control locations for the tokenized securities of a broker-dealer's customers. To rely on a transfer agent as a good control location for its customers' tokenized securities, a broker-dealer would need to hold its customers' securities in compliance with the terms of a no action letter permitting a transfer agent to be a control location. That letter provides that a transfer agent can be a good control location for a broker-dealer's customers' securities under the following conditions:

- The broker-dealer carries the tokenized securities "long" in customers' accounts;
- The broker-dealer reflects separately all customer tokenized securities positions in securities records or ledgers pursuant to Rule 17a-3 under the Exchange Act;
- When accepting custody of the tokenized securities, the broker-dealer is not aware of any substantial problems of an operational nature that the issuer of those tokenized securities may be experiencing and which may endanger the interests of the customer;
- The broker-dealer obtains written assurance that the tokenized securities are not subject to any right, charge, security interest, lien, or claim of any kind in favor of the transfer agent or any person claiming through transfer agent;
- The tokenized securities are registered with the Commission pursuant to the Securities Act of 1933, exempt from registration, or not required to be registered; and
- The broker-dealer will maintain in a separate file a current list of all investments of tokenized securities that are carried on its books and records subject to the terms and conditions set forth above.[71]

Using a transfer agent to establishing control of tokenized securities for purposes of Rule 15c3-3, the books and records of a broker-dealer holding customer tokenized securities would show those securities as carried long in the customer's account with the broker-dealer, just as they would when establishing the equivalent of physical possession. The broker-dealer would hold its customers' tokenized securities in wallets that it establishes and for which it holds the private keys. The broker-dealer would have to ensure that the transfer agent shows the broker-dealer as the legal owner of the tokenized securities that the broker-dealer carries for its customers. The broker-dealer's books and records would show the customers as the beneficial owners of

70 The Staff has recognized that the following can be good control locations for uncertificated securities: the general partner of a limited partnership (SEC Letter to Wayne Hummer & Co. (Mar. 6, 1986) and SEC Letter to Wilmer, Cutler & Pickering (July 30, 1997)); the designated manager of limited liability company (SEC Letter to Wilmer, Cutler & Pickering (Sept. 17, 1999)); and the contractual adviser to a REIT (SEC Letter to Holland & Knight, LLP (Jan. 18, 2000)).

71 SEC Letter to Sanford C. Bernstein & Co (June 9, 2009), https://www.sec.gov/divisions/marketreg/mr-noaction/2009/bernstein090809.pdf.

those securities.

A broker-dealer would perform a reconciliation to demonstrate its control of customers' tokenized securities. It would reconcile the amount of a digital security shown on the books and records of the transfer agent for that security with the aggregate amount of that security held in customer wallets, which amount can be verified on the blockchain. The broker-dealer would then compare the transfer agent records and wallet holdings for the digital security with the aggregate amount of that security that it carries in the accounts of all its customers, as reflected on its books and records. The amount of the digital security on the books and records of the transfer agent, in customer wallets, and held in customer accounts in aggregate should match. We understand that an auditor could verify that tokenized securities are held in a wallet by requiring a broker-dealer to transfer a small amount of securities held in that wallet to a wallet designated by the auditor, or by requiring a broker-dealer to sign a message from that wallet. This would allow the auditor to verify that the broker-dealer controls the private keys for that wallet.

State-chartered trust companies arguably should be permitted to serve as control locations for tokenized securities. We understand that the financial services agencies of certain states have permitted trusts to hold various types of crypto assets, including tokenized securities. The SEC, however, would have to designate state-chartered trusts as good control locations under paragraph (c)(7) of Rule 15c3-3. It is unclear whether the SEC is prepared to designate entities, such as trusts, that are not subject to federal supervision as good control locations.

D. CUSTODY – INVESTMENT ADVISERS

Rule 206(4)-2 (commonly referred to as the "Custody Rule") under the Investment Advisers Act of 1940 (the "Advisers Act") establishes certain safekeeping requirements applicable to funds or securities held on behalf of clients by registered investment advisers.[72] Although the Custody Rule applies only to registered investment advisers, its concepts are relevant for non-registered advisers as well, since clients of those advisers still have a practical interest in assuring that managed assets are appropriately safeguarded and the absence of appropriate custody arrangements may preclude a client from investing with a particular adviser.

1. SCOPE OF THE CUSTODY RULE

On its face, the Custody Rule applies to the custody of client "funds or securities". Digital assets can be characterized in a number of ways. Since the SEC has taken the view that such tokenized securities constitute securities for purposes of the U.S. federal securities laws,[73] and since the SEC has not provided any interpretations or guidance to the contrary, it would seem

72 17 C.F.R. § 275.206(4)-2.
73 *See* Munchee Inc., *supra* note 9.

that security tokens would fall within the scope of the Custody Rule. In fact, a March 2019 letter to the President of the Investment Advisers Association from Paul G. Cellupica, Deputy Director and Chief Counsel of the SEC's Division of Investment Management, demonstrates that the SEC is continuing its efforts to engage with market participants and better understand how characteristics of digital assets impact the application of the Custody Rule.[74]

2. PURPOSES OF THE CUSTODY RULE

While appropriate custody arrangements can provide protections against inadvertent loss or theft by third parties, another key purpose of the Custody Rule is to protect against fraud or misconduct on the part of an adviser or its employees or representatives. So, broadly speaking, custody through an independent third party might be viewed as providing (or at least aimed at providing) three key protections:

- Protection against theft or misappropriation by third parties
- Protection against bankruptcy or insolvency of the adviser or custodian (i.e., by segregating the assets and identifying them as being held on the client's behalf)
- Protection against fraud, theft or misappropriation by the adviser itself

3. SUMMARY OF CUSTODY RULE REQUIREMENTS

Unless certain exceptions apply (which may make all or part of the Custody Rule inapplicable to certain securities or in certain situations), an investment adviser that is registered or required to be registered under the Advisers Act is required to comply with certain requirements if it has custody of client funds or securities. Among such requirements are the following: [75]

Qualified Custodian: Funds or securities held on behalf of clients must be maintained by a "qualified custodian".

Each of the following is a "qualified custodian" under the Custody Rule:

- A bank as defined in section 202(a)(2) of the Advisers Act[76] or a savings association as defined in section 3(b)(1) of the Federal Deposit Insurance Act that has deposits insured by the Federal Deposit Insurance Corporation under the Federal Deposit

74 Letter from Paul G. Cellupica, Deputy Director and Chief Counsel, Div. of Inv. Mgmt., Sec. & Exch. Comm'n. to Karen Barr, President and CEO, Inv. Advisers Ass'n (Mar. 12, 2019); *see also* Beagan Wilcox Volz, SEC Asks Industry How to Best Custody Crypto Assets, IGNITES.COM (Mar. 15, 2019).

75 *See* 17 C.F.R. § 275.206(4)-2(a).

76 In addition to federally-chartered banks, other member banks of the Federal Reserve System and certain other identified identities, the definition of "bank" for this purpose includes a state-chartered or federally-chartered trust company if a substantial portion of the business of such trust company consists of receiving deposits or exercising fiduciary powers similar those permitted to national banks. If a trust company is formed and operated solely for the purpose of providing custody services, a legitimate question might be raised as to whether such custody services are fiduciary in nature. Paul G. Cellupica, Deputy Director and Chief Counsel of the SEC's Division of Investment Management, may have been alluding to this potential issue when he asked (in a March 2019 letter addressed to the Investment Adviser Association) whether advisers have experienced similarities or differences in custodial practices of trust companies as compared to those of banks and broker-dealers. Letter from Paul G. Cellupica, Deputy Director and Chief Counsel, Div. of Inv. Mgmt., Sec. & Exch. Comm'n. to Karen Barr, President and CEO, Inv. Advisers Ass'n (Mar. 12, 2019).

Insurance Act

- Registered broker-dealers holding client assets in customer accounts
- Registered futures commission merchants holding client assets in customer accounts (but only with respect to clients' funds and security futures, or other securities incidental to transactions in contracts for the purchase or sale of a commodity for future delivery and options thereon)
- Foreign financial institutions that customarily hold financial assets for their customers, provided that the foreign financial institution keeps the advisory clients' assets in customer accounts segregated from its proprietary assets.[77]

Notice to Client: Notice must be provided to clients if an account is opened with a qualified custodian on a client's behalf.

Account Statements: The adviser must have a reasonable belief that the qualified custodian is sending account statements to the client (or, in the case of a client that is a pooled fund or similar investment vehicle, the underlying investors in the pooled vehicle) at least quarterly.

Verification and Surprise Audit: The funds and securities held in custody must be verified at least once during any calendar year, generally by an independent public accountant. The examination and verification must be at a time chosen by the accountant without prior notice or announcement to the adviser or the custodian and must be a time that is irregular from year to year.

4. SELF-CUSTODY

The Custody Rule does not preclude self-custody by a registered investment adviser. However, the adviser or its "related person" that maintains actual custody of client funds or securities must itself be a qualified custodian.

In those circumstances, certain additional requirements generally apply. First, the independent public accountant retained to satisfy the surprise audit requirement must be registered with, and subject to regular inspection by, the Public Company Accounting Oversight Board (PCAOB) in accordance with its rules. Second, a written internal control report must be provided within six months of becoming subject to the Custody Rule and at least once per calendar year thereafter. The internal control report must be prepared by an independent public accountant and must include an opinion of a PCAOB-registered independent public accountant as to whether controls have been placed in operation as of a specific date and are suitably designed

77 *See* 17 C.F.R. § 275.206(4)-2(d)(6).

and are operating effectively to meet control objectives relating to custodial services, including the safeguarding of funds and securities held on behalf of the advisory clients, during the relevant year. Such independent public accountant must also verify that the funds and securities are reconciled to a custodian other than the registered investment adviser or its related person.

5. PRACTICAL IMPACT AND CONSIDERATIONS

Certain third-party service providers have begun providing digital asset custody services to investors in the space. In order to broaden their potential client base, certain of such service providers have actively sought to take steps to establish "qualified custodian" status. For example, certain service providers have acquired existing trust companies and broker-dealers or taken steps to establish a state-chartered trust company.[78]

There are a number of practical difficulties that may still need to be overcome with respect to the provision of custody services in a manner consistent with the purposes of the Custody Rule:

- ***Limits on Scope of Custody Services:*** Unlike typical broker-dealer arrangements, where one security is readily tradable for another security or cash and the proceeds of a transfer or sale can be received and held by the broker-dealer in the brokerage account on a "payment versus delivery" basis, typical current cryptocurrency custodians only provide for custody of a limited number of approved cryptocurrencies. They may or may not have the capability to hold cash for a client. They almost certainly will not agree to hold any and all cryptocurrencies in which a client may choose to invest. Without a significant expansion of the number and types of cryptocurrencies that may be held with a particular custodian, the practical ability of advisers to trade broadly in cryptocurrency investments may be limited.

- ***Audit Difficulties:*** It remains to be seen whether typical independent accountants will be willing to provide the surprise audits required by the Custody Rule. There are certainly some accounting firms that have taken an active interest in the digital asset space. But, without additional guidance from the SEC or accounting standards boards, accountants may have difficulty confirming that a private key held by a custodian actually represents an ownership interest in the particular underlying digital asset. Unlike typical investments in securities and debt instruments, there are no registrar records, trusted securities intermediaries, trusted counterparties, administrative agents or other traditional sources of ownership verification. Verifying ownership of digital assets may require technical expertise and knowledge that may not be readily available at this point to typical accounting firms.

78 *See, e.g.*, Press Release, N.Y. Dep't of Fin. Services, DFS Authorizes Coinbase Global, Inc. to Form Coinbase Custody Trust Company LLC (Oct. 23, 2018), https://www.dfs.ny.gov/about/press/pr1810231.htm; Ben McLannahan, Wall Street starts to dip its toes in crypto Fin. Times (Aug. 13, 2018), https://www.ft.com/content/db5a20ea-9ca1-11e8-9702-5946bae86e6d; Kate Rooney, Companies Race to Solve Bitcoin's Security Problems Despite Slumping Prices, CNBC (Sep. 13, 2018), https://www.cnbc.com/2018/09/13/companies-race-to-solve-bitcoins-custody-problem-despite-slumping-prices.html.

» ***Adviser Fraud Risk:*** While current custody methods can provide significant protections against hacking and other cyber threats involving third parties, it is not clear that such methods will satisfy the goal under the Custody Rule of providing substantial protections against adviser fraud or misappropriation of assets. A custodian of digital assets primarily serves as a secure storage point for those assets. However, in the context of providing custody for assets managed for an investment vehicle or other ultimate client by an investment adviser, the custodian basically acts at the instruction of the adviser. If the adviser wants to transfer digital assets out of custody and does so in accordance with established procedures, the digital assets can leave the custody arrangement without cash or other replacement assets being received by the same custodian. Such transfers can occur relatively quickly, and an adviser may be able to abscond with digital assets or the proceeds thereof in quick order. It is possible, of course, that digital assets that are traced back to a fraudulent transaction can be blacklisted in some manner—which may limit trading of those assets going forward. However, this has the potential to harm innocent recipients of proceeds of the fraudulent transaction (i.e., those who had no knowledge that the original digital assets were misappropriated). It also may not be a significant deterrent to a large theft by an adviser, who can quickly exchange digital assets for cash and abscond with the cash before any custodian or digital asset exchange has knowledge of any wrongdoing.

Solving for these difficulties has implications beyond tokenized securities complying with the custody rules of the federal securities laws. Custody has been identified as an important issue in the larger efforts of institutional actors to adopt digital assets. In her January 2018 letter to two industry groups, Dalia Blass, the Director of the SEC's Division of Investment Management, identified the issue of custody and the custody requirements of the Investment Company Act of 1940 as necessary elements to address if the SEC is to approve an exchange-traded fund that invests in digital assets.[79]

V. PRINCIPLES AND GUIDELINES FOR SECURITIES TOKEN SPONSORS AND TRADING PLATFORMS

Given the increase in interest in securities tokens, the following points highlight a few key issues that require careful consideration before issuing a securities token or trading it on a platform.

TOKEN ISSUERS:

» Issuers must comply with registration requirements under the U.S. securities laws in issuing tokenized securities. Such securities either must be issued under a recognized exemption to registration or be

79 Letter from Dalia Blass, Director, Div. of Inv. Mgmt., Sec. & Exch. Comm'n. to Paul Schott Stevens, President and CEO, Inv. Co. Inst. (Jan.18, 2018), https://www.sec.gov/divisions/investment/noaction/2018/cryptocurrency-011818.htm.

registered. Each regime – whether fully registered or issued pursuant to an exemption – carries specific obligations and limitations, both at the outset of issuance and ongoing. The pros and cons of each will drive the determination of which option to use and are described in the Chart to this Chapter and more fully in Appendix A.

- Issuers of tokenized securities also may wish to issue utility tokens (for example, the securities token is used to raise funds, but the utility token will be used on the platform). An issuer may want to issue securities that exist temporarily until it can issue a utility token, or the issuer may wish to issue utility tokens in addition to securities tokens. Whether an issuer wishes to maintain one more classes of securities will determine whether it issues a tokenized security in the form of placement tokens, mutable tokens, or dividend-paying tokens. Each type of securities token brings varying levels of regulatory complexity, and each must be considered before issuing the token to ensure the model meets the needs of the platform and the business.
- Entities that issue tokens overseas must still be cognizant of U.S. securities laws, given the digital nature of the token and its ability to be issued and traded across borders. Moreover, a token that does not qualify as a security in one country may still be considered to be a security in the United States. Issuers must take precautions to ensure they comply with relevant exemptions or otherwise do not trigger U.S. law.

TOKEN TRADING PLATFORMS:

- Tokenized securities need secondary markets to provide liquidity to purchasers of such securities. Such securities will likely trade on a registered national securities exchange or an ATS. ATS are subject to a lighter regulatory touch and shorter application process, but national securities exchanges have the ability to list securities for trading and generate data fees.
- The nature of digital assets that qualify as securities introduces new considerations for broker-dealers attempting to meet securities law requirements. The below discussion has not been endorsed by the SEC and should be reviewed with legal counsel prior to implementing:

    a. **Physical possession.** Broker-dealers must maintain the equivalent of physical possession of their customers' securities tokens for purposes of Rule 15c3-3 under the Exchange Act. This could arguably be accomplished by holding them in wallets for which the broker-dealer holds the private key and by engaging an auditor to verify holdings.

    b. **Control.** Alternatively, broker-dealers must establish control of its customers' securities tokens for purposes of complying with Rule 15c3-3 under the Exchange Act. This could arguably be accomplished by using a transfer agent to establish the legal owners of such securities, coupled with engaging auditors to verify holdings. Nevertheless, this solution introduces additional

intermediaries that blockchain sought to streamline.

c. **Control Locations.** Rule 15c3-3 permits a bank to serve as a control location for customers' tokenized securities, but federal banking regulators have yet to approve banks to hold crypto assets. Some state financial regulators have approved state-chartered trusts to hold tokenized securities, but the SEC has to issue guidance permitting such trusts to serve as good control locations for purposes of Rule 15c3-3. Neither the SEC nor its staff has issued guidance on how broker-dealers may comply with Rule 15c3-3, however.

INVESTMENT ADVISORS:

» An SEC-registered investment adviser must hold tokenized securities in compliance with the SEC's Custody Rule, Rule 206(4)-2 under the Advisers Act. An investment adviser must hold such securities in a financial institution identified by the rule, and the adviser must conduct due diligence to ensure that it receives the range of custody services the adviser requires.

VI. CONCLUSION

Tokenized securities have many unique characteristics that offer dramatic improvements over traditional securities, but those involved in issuing or trading tokenized securities must understand and comply with regulations that were developed and designed for traditional securities. For instance, there are a number of special considerations for securities offerings with utility token features. In many cases, the application of existing regulations raises unique issues that will require policymakers and regulators to issue new guidance. This paper has addressed a number of key issues that should be carefully considered.

IV. CHAPTER 2: CONSIDERATIONS AND GUIDELINES FOR UTILITY TOKENS

DATED AS OF JULY 30, 2018[80]

SECTION 1: PRINCIPLES AND GUIDELINES FOR TOKEN SPONSORS

INTRODUCTION

This Section[81] provides introductory principles and guidelines for Token Sponsors as a way to promote sound business practices. Within the context of this report, a "**Token Sponsor**" or "**Sponsor**" is any clearly defined individual or group that (a) generates or distributes, or (b) undertakes to lead or control the development, adoption, or distribution of, a digital token that is not intended to be a security or CFTC Regulated Instrument. For these purposes, the activities of a Token Sponsor inherently entail more than the development and publication of a blockchain protocol that uses tokens. Hence, not all digital tokens are generated through the efforts of a Token Sponsor — indeed, bitcoin was generated independent of a Token Sponsor.

Digital tokens can take a variety of forms and serve many purposes. This Section provides principles and guidelines for Token Sponsors to manage the risk that the offering and distribution of a digital token may run afoul of certain federal securities and commodity laws by (a) discussing why a digital token may become subject to certain securities and commodities laws and regulations, (b) presenting steps that may reduce the risk of the token being treated as a security or a CFTC Regulated Instrument, (c) explaining a suggested path for Token Sponsors to follow when launching a digital token, and (d) offering guidelines for drafting token projects' white papers and other marketing materials.

TOKEN SPONSOR

Any clearly defined individual or group that (a) generates or distributes, or (b) undertakes to lead or control the development, adoption, or distribution of, a digital token that is not intended to be a security or CFTC Regulated Instrument (as defined above in Part 1).

80 This Chapter was published on July 30, 2018 as Part 2: Considerations and Guidelines for Utility Tokens in Understanding Digital Tokens: Market Overviews and Proposed Guidelines for Policymakers and Practitioners (July 2018), https://digitalchamber.org/token-alliance-whitepaper/.

81 These principles and guidelines apply within U.S. securities and commodity regulatory regimes.

I. WHEN IS A DIGITAL TOKEN SUBJECT TO REGULATION BY THE UNITED STATES SECURITIES AND EXCHANGE COMMISSION OR COMMODITY FUTURES TRADING COMMISSION?

CHARACTERISTICS OF A SECURITY

United States federal securities laws define "security" broadly. A digital token that demonstrates ownership of an instrument enumerated in these definitions, such as a note or other evidence of indebtedness, share of stock, or undivided fractional interest in mineral rights, would typically be subject to regulation by the SEC under the federal securities laws and by state authorities under their "blue sky" laws.

Although the application of United States federal securities laws and related regulations to particular situations, including interpretations by courts, emphasizes the underlying substance of a transaction, Token Sponsors must be cognizant of confusion that might arise in the marketplace from their use of imprecise or inapposite terminology. If a digital token is not intended to be a security, then it is advisable to avoid using securities-related terminology in white papers and other marketing materials that may confuse readers as to the nature of the token. Examples may include statements such as:

- Token holders will "own" or "profit" from a blockchain or network;
- Token holders will receive "interest" or "dividends" on their tokens; or
- References to the token's "market capitalization" or "market cap."

Even referring to an "initial coin offering" or "ICO" may invite comparison to an initial public offering of securities.

THE *HOWEY* TEST

Digital tokens may trigger United States federal securities laws if they are an "investment contract" – a catchall for securities that are not otherwise set out in the definition of a "security." The test for whether any instrument is an "investment contract" under the United States federal securities laws[82] is commonly referred to as the "*Howey* Test." Stemming from a 1946 Supreme Court case of the same name,[83] the *Howey* Test holds an investment contract to exist if there is:

82 For the purposes of these Principles and Guidelines, "U.S. federal securities laws" refers to the Securities Act and the Exchange Act.
83 *SEC v. W.J. Howey Co.*, 328 U.S. 293 (1946).

THE HOWEY TEST AN INVESTMENT CONTRACT EXISTS IF THERE IS:

1	2	3	4
AN INVESTMENT OF MONEY	IN A COMMON ENTERPRISE	REASONABLE EXPECTATION OF PROFITS	PROFITS DERIVED FROM THE SUBSTANTIAL EFFORTS OF OTHERS

*BASED ON 1946 SUPREME COURT CASE SEC V. HOWEY

All four elements of the *Howey* Test must be met for an instrument (such as a token) to be considered an investment contract. Form and nomenclature hold no weight, rather it is the substance of the instrument in question that is important. **Thus, it is important for Token Sponsors to have an attorney expert in United States federal securities laws analyze the application of the *Howey* Test to a Token Sponsor's proposed digital token before the token is offered or distributed. This includes any form of distribution, including system-based rewards, "airdrops," and distributions to employees, founders, contractors, and consultants.**

COMMODITY REGULATION

The CFTC may exercise general anti-fraud and anti-manipulation authority over any digital token it deems to represent a "commodity," as broadly defined under the Commodity Exchange Act. Moreover, any arrangement that involves the future delivery of a digital token may subject the arrangement or the token to regulation by the CFTC as a futures agreement, swap, option to buy or sell the token, or retail commodity transaction, which are defined as "**CFTC Regulated Instruments**."

It thus should be a common practice for the Token Sponsor's legal counsel also to consider whether a digital token may create a CFTC Regulated Instrument under the CEA, or the impression of such an instrument. Even when this is not the case, working with counsel to conduct such analyses may provide valuable guidance regarding how the digital token should be distributed in compliance with the CFTC's anti-fraud and anti-manipulation regulations.

II. HOW CAN A TOKEN SPONSOR MANAGE THE RISKS OF HAVING A DIGITAL TOKEN TREATED AS AN INVESTMENT CONTRACT OR CFTC REGULATED INSTRUMENT?

Ultimately, there is no better means of assisting a Token Sponsor in complying with SEC and CFTC regulations than a candid assessment by experienced legal counsel of the token's intended uses and

the means by which the tokens will be generated, offered, and distributed. This assessment should be updated as circumstances of the digital token change and the regulatory landscape evolves.

The SEC, CFTC, and United States courts will consider all relevant facts and circumstances when considering whether a Token Sponsor's activities entail the offering or sale of an investment contract or a CFTC Regulated Instrument. Although the SEC's and CFTC's positions regarding digital tokens are evolving, the following factors may reduce the risk of a digital token becoming subject to such regulations.

- **Full development of requisite system(s) and/or application(s) before distribution:** A digital token distributed by a Token Sponsor should be one component of fully-developed system(s) and/or application(s) designed by a Token Sponsor. Upon distribution, the token should provide access to any affiliated services or applications. Otherwise, the Token Sponsor's continued development efforts may be (i) viewed by the SEC as efforts from which token holders reasonably expect to profit, or (ii) viewed by the CFTC as a promise for the delivery of a commodity at a future date.
- **Timing of the distribution of a digital token:** A Token Sponsor should not deliver its digital token to purchasers until everyone who receives tokens can use them to access applicable system(s) and/or application(s), unless expert counsel confirms that the token can be delivered at an earlier point in compliance with applicable SEC or CFTC regulations.
- **Tokenized commodities should be accessible:** If a Token Sponsor's digital token is designed to represent ownership interest in a specified commodity (including another token), the digital token should be related to a system or application that is able to provide token holders with timely access to the specified commodity. A token designed to adjust in price in response to the price, or change in price, of a commodity without entitling the token holder to obtain or control a corresponding amount of the commodity may viewed by the CFTC as a CFTC Regulated Instrument.
- **Token holders should not sell digital tokens on credit:** Selling digital tokens on credit, requiring purchasers to post collateral, or otherwise providing a leveraged exposure to the token or any underlying commodity may qualify as a CFTC Regulated Instrument. A delay of more than 28 days between the agreement to purchase a token and its delivery to the purchaser may increase this risk.
- **Focus communications on the value of using the digital token:** While a Token Sponsor will want users of its digital token to understand and appreciate the potential value of the token's project, the Token Sponsor should seek to be clear that the digital token is not intended to provide a passive investment opportunity for its holders. This may be aided by the Token Sponsor emphasizing the benefits of using or consuming the digital token and emphasizing any ways in which token holders and other network participants will contribute to the token's potential value.
- **For financial and accounting purposes, treat the digital token consistently with its use:** When permitted by generally accepted accounting principles, tax regulations, and similar rules, the treatment

and discussion of the digital token in the Token Sponsor's financial statements, reports and analyses should be consistent with its use in the related systems or applications. Characterizing the digital token as an investment, security, or CFTC Regulated Instrument for tax and accounting purposes could influence its regulatory treatment by the SEC or CFTC. This is not to suggest, however, that the use of a term mandated by tax or accounting rules, such as "forward contract" for example, would be considered dispositive as to the character of a digital token or contract relating to the token for purposes of SEC or CFTC regulations – only that it may give the appearance of inconsistent treatment.

» **Tokens should be designed so that holders do not expect profits from the token's project:** Projects should not entail equity rights and should not result in the periodic distribution of funds (whether fiat or crypto-currency) to digital token holders, or the expectation of such distributions. Likewise, a Token Sponsor should not design or market digital tokens with any emphasis on price-appreciation or profit delivery to token holders. In particular:

- A Token Sponsor should try to avoid hallmarks of a traditional security, such as (1) a stake of ownership or control in a company or venture behind a digital token project (including a decentralized autonomous organization), or (2) the sharing of any of a Token Sponsor's profits with other token holders through distributions, dividends, interest, or other payments.
- A Token Sponsor should be wary of features in the digital token that would be reasonably expected by a prospective purchaser to cause the token to appreciate in price or otherwise provide passive returns to the token holders.
- A Token Sponsor should be cautious in using the digital tokens as financial incentives for employees or others, so as to avoid the appearance that these recipients reasonably expect the token to appreciate in price.

Distributions of a digital token before the underlying project for the token is complete can be at risk of creating investment contracts even if the token would not be subject to federal securities laws once the project is fully completed. Selling tokens at a discount to a projected public sale price or to raise funds for the project may contribute to this risk. In order to successfully conduct a pre-sale, a Token Sponsor may need to ensure compliance with the registration requirements or an exemption from registration under the Securities Act and delay delivery of the token until the project is constructed and fully functional.

When practical, a Token Sponsor may choose to fully comply with an applicable exemption from registration, including limiting the type of persons (such as accredited investors or eligible contract participants) to which its token is sold or the jurisdictions in which an offering is conducted, rather than rely on arguments for why the token should fail the *Howey* Test. Compliance with such an exemption should not prevent a Token Sponsor from subsequently concluding that its digital token does not qualify as an investment contract and permitting the digital token to be transferred without compliance with the exemption.

III. WHAT ARE THE STEPS FROM INCEPTION TO COMPLETION OF A DIGITAL TOKEN DISTRIBUTION?

A Token Sponsor should follow the steps set forth below, as applicable, when launching a digital token that is intended to be neither a security nor a CFTC Regulated Instrument. Following the order of the steps below is important, as any action taken out of order may compromise the regulatory standing of the token:

Concept and technology development: A Token Sponsor should fully develop its conception of its underlying system(s) and application(s) employing the digital token. This primarily includes the development of clear frameworks related to: (i) how the system will enable the provision of any applications, products, and/or services to which the token will provide access, (ii) the design and construction of any related external facing applications, and (iii) the writing and testing of code.

White paper and other materials: A Token Sponsor should draft a complete and accurate white paper, which should be reviewed by expert legal counsel before publication (including posting on a website or social media). Please refer to Section D of these Principles and Guidelines for Token Sponsors for more information on what, at a minimum, should be included (and excluded) from a white paper. It is recommended that, when appropriate, separate materials should be prepared to address how the token will be offered and distributed to users.

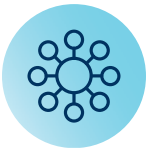
Regulatory review: The Token Sponsor, with counsel, should review its token project, its accompanying white paper, and any related applications, services, or marketing materials for issues related to state and federal money transmitter laws, import and export regulations, AML/OFAC compliance obligations, federal and state securities laws, commodity laws, and any other potential legal or regulatory considerations related to the sponsor's specific business. In particular, they should consider:

- The application of the *Howey* Test and other aspects of the definition of a "security" to the digital token;
- Whether a Token Sponsor's digital token involves a CFTC Regulated Instrument like a swap or retail commodity transaction;
- Tax and related reporting requirements that may arise from the creation and distribution of the token and the operation of the applications related to the token;

- Whether to register with FinCEN as a "money services business";
- Whether to conduct appropriate "know your customer" activities in relation to the distribution of the token to comply with any applicable money laundering, OFAC, and/or import/export laws; and
- Whether to consult with legal counsel in other jurisdictions.

Corporate review (*if appropriate for the token*): The Token Sponsor should establish all necessary corporate or other legal entities (which may include the drafting of corporate governance documents, board resolutions, etc.), register intellectual property, draft privacy policies and user terms, and prepare external communications strategies. The Token Sponsor should seek counsel to work on any transactions to raise capital for the project apart from a potential pre-sale.

Pre-utility sale (if appropriate for the token): A Token Sponsor may need to sell (but not deliver) digital tokens in advance of completion of the associated system(s) or application(s). This may require the Token Sponsor to sell the digital tokens in compliance with an exemption from the Securities Act and the CEA, even though the Token Sponsor does not anticipate that its digital tokens will qualify as securities or CFTC Regulated Instruments after the system(s) and application(s) are completed. The Token Sponsor should seek expert legal counsel to assess whether the sale requires an exemption and, if so, what exemptions would be available. If an exemption is required, legal counsel should assist the Token Sponsor in developing and executing a legal and regulatory compliance program relating to the pre-utility sale.



Public distribution: The Token Sponsor should develop and complete a token distribution closing checklist designed to ensure compliance with applicable laws and regulations. Also, if the Token Sponsor's planned token distribution so requires, counsel should assist the Token Sponsor in drafting appropriate terms and conditions, including representations and warranties, as well as any agreement that will govern the distribution.

IV. WHAT MINIMUM INFORMATION SHOULD BE INCLUDED IN A DIGITAL TOKEN'S MATERIALS?

Digital tokens generally have accompanying materials such as a white paper and marketing materials. A Token Sponsor that intends to generate and distribute a digital token should draft a clear and complete white paper explaining the relevant facts related to the token project, its utility and value proposition as well as any problem(s) it seeks to solve, any related products and/or services, and how the token

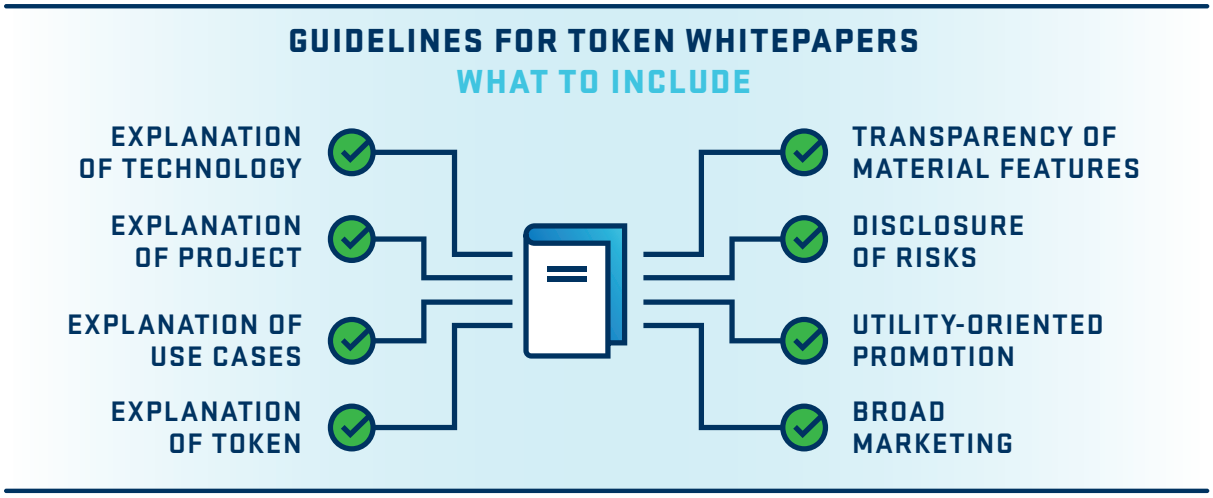
is intended to operate as an integral part of the project. Additionally, marketing materials themselves can come in many forms, both written and spoken. Marketing materials in any form should be crafted carefully. A clear division of labor can be helpful, with the white paper and certain other information focused on how people can use the token and other materials focused on how and why people should acquire tokens.

SPONSORS SHOULD MARKET A PRODUCT RATHER THAN AN INVESTMENT

Marketing materials should focus on the benefits of using the token for its intended application and be addressed to those likely to use the token in this manner. For example, if a token could only be used by members of a network, purchasers should be required to join the network before receiving their tokens. Marketing efforts should not be directed at those known to be in the business of or making a practice of recommending or purchasing tokens as investments.

INFORMATION THAT SHOULD BE INCLUDED IN A WHITE PAPER

A Token Sponsor's white paper is a critical document. A white paper provides background on a Sponsor's token project, as well as specifics on the project's technological application, any related products or services, and how the digital tokens will operate. If the tokens are designed to monetize the value of such products or services, it may be appropriate to explain the business model underlying the project. A white paper is not a business plan, marketing materials, offering memorandum, or prospectus – it is a factual description of how the token will operate as part of a system or within an application. The white paper will often form the objective basis for evaluating the regulatory implications of the projects, including the distribution of the tokens and the offer of any products, applications, and services. Thus, Token Sponsors should carefully consider what should and should not be included in their white papers.



- **Explanation of Technology:** A Token Sponsor's white paper should explain the technology underlying the token project's token and affiliated system(s) and/or application(s). It might include such matters as a description of the underlying code, how an application interacts with the platform, why a blockchain-based product or service is critical to solving the problem(s) that the token project aims to address, and the operation of the token network. Any means by which the token's protocol enables control of, changes to, or corrections of the token's protocol should be discussed. Depending on the intended token recipient, the Token Sponsor should carefully separate hyper-technical or dense discussions of the technology from plain-language discussions of the technology to enable the widest possible audience to understand the project and its central components. While technical discussions of the technology may be very important, a Token Sponsor should consider including them as appendices to, or separate documents from, the project's white paper.

- **Explanation of Project:** A Token Sponsor's white paper should explain the utility of the token project and include a description of how the project seeks to achieve its intended purpose as well as how the token will be used for this purpose.

    - **Services and Products:** A white paper should describe system(s) or application(s) that may be acquired or utilized with the token.

    - **Use of Smart Contracts:** If the Token Sponsor's project uses smart contracts, the white paper should describe how the smart contracts are intended to be used, what purposes they are intended to serve within the application, and how the smart contracts are intended to operate, including how they self-execute in the context of the application.

- **Explanation of Use Cases:** A Token Sponsor's white paper should consider providing current use cases for the project's products and/or services and specifically the digital token. The explanation can include descriptive or illustrative case studies of the application to provide the reader an understanding of how the project's application and token will work in practice within the blockchain application.

- **Explanation of Token:** A Token Sponsor's white paper should provide a comprehensive description of a token that is imbedded in the product and/or service. The description should include the form of the token (*e.g.*, ERC20, etc.), and any rights of, or benefits to, and obligations of, token holders.

- **Transparency of Material Features:** A Token Sponsor, through published material or statements (such as a white paper and distribution terms), should transparently disclose the material features of its digital token and of the token's distribution, including information pertaining to pricing, structure, allocation, and utility.

- **Disclosure of Risks:** A white paper should disclose any foreseeable conditions that could disrupt or impair use of the tokens' application(s) or system(s). If the Token Sponsor has devised plans to mitigate certain risks, it should disclose the material details of such plans.

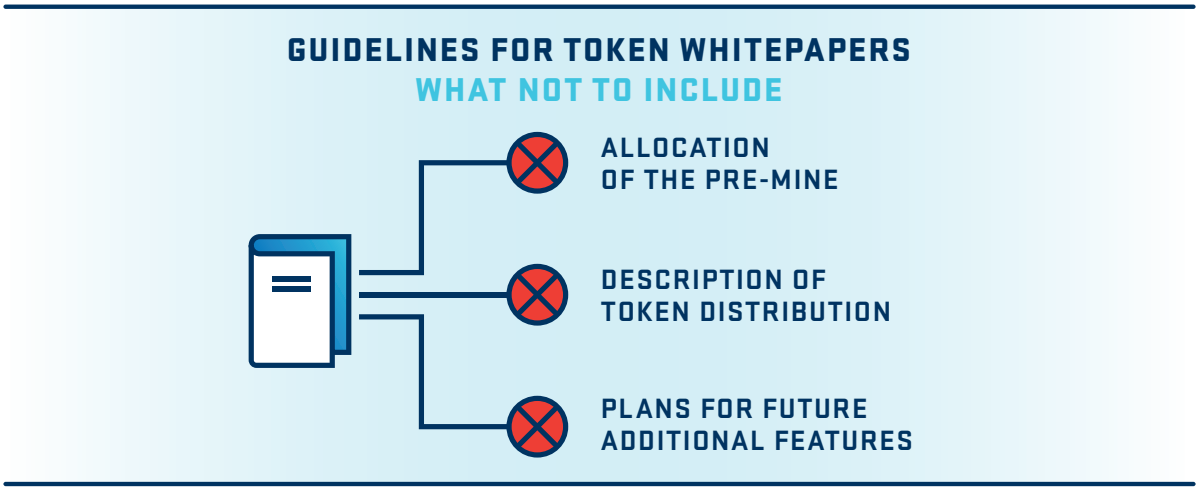
» **Utility-Oriented Promotion:** Promotion of the system or application for a Token Sponsor's digital token should not encourage interest in acquiring the token based solely on investment expectations or a fear of missing out on an investment. Depending on other facts, such promotion could affect the token's characterization as a security. The Token Sponsor should not link to or reference material the content of which is not in its control.

» **Broad Marketing:** The dissemination of a Token Sponsor's white paper should be focused towards the population who would most likely use or benefit from the Token Sponsor's product, service, or token. The marketing of a white paper should not be targeted toward general populations with an interest in investing, particularly those who speculatively invest in digital tokens, or who buy with the sole intention of selling for increased returns.

INFORMATION THAT SHOULD NOT BE INCLUDED IN A TOKEN SPONSOR'S WHITE PAPER

» **Allocation of the pre-mine:** A Token Sponsor's white paper should avoid discussion of any allocation of tokens for investors, developers, founders, or employees. Such discussions would appear to be more relevant to a potential investor in the project than a user of the application.

» **Plans for future additional features:** A Token Sponsor's white paper should not discuss any plans that the Token Sponsor may have for expanding the features or scope of the project's products, services or applications, or other proposed enhancements to the token's use after the launch of its token. Emphasis on plans for future development by the Token Sponsor may negatively affect a digital token's security analysis under the *Howey* Test.



» **Description of the distribution of tokens:** If a Token Sponsor's digital token will be distributed in private sales, a limited public sale or auction, airdrop, or a similarly limited event, it may be more appropriate to describe the event in separate materials that can be superseded when the event is

completed, rather than in the Token Sponsor's white paper. Such materials may include details that would only be of interest to participants in the event. This may help keep readers from improperly regarding a Token Sponsor's white paper as marketing the token rather than describing its operation.

Of course, a Token Sponsor's white paper generally should discuss any means its system(s) or application(s) employ to distribute tokens as part of its regular operations. Such systemic distributions might include rewards for work done in generating or verifying new blocks and rewards for other work done to operate the system(s) or application(s).

INFORMATION THAT SHOULD NOT BE INCLUDED IN A TOKEN SPONSOR'S PROMOTIONAL AND MARKETING MATERIALS GENERALLY

- **Intentional misrepresentations or misleading statements:** A Token Sponsor should not make any misrepresentations, misleading statements, or omit any material facts that could be deemed important information for someone using or acquiring its digital token.
- **Promises of financial returns:** A Token Sponsor should take care that materials relating to its digital token not make statements that characterize the token as a passive investment opportunity or imply that the token holders will earn financial gains as a result of business activities of the Token Sponsor unrelated to the underlying utility of the tokens' system(s) and application(s). Examples of such statements are those made in the *Munchee* Order regarding how the "ecosystem" had been designed to cause the token to appreciate or, as discussed in more detail in Section 2, the prospects for a secondary market. Token Sponsors should avoid making promissory statements.
- **Discussion of matters that might primarily interest investors:** A Token Sponsor's materials should not make any statements that would be relevant to an investor but not to a user of the application(s) or system(s) relating to the digital token. Quantitative statements regarding current or potential markets for such application(s) or system(s) should be carefully considered. The user of a digital token to obtain a service, for example, may find the number of customers or the number of times the service is accessed more relevant than the dollar amount spent on the service. Sponsors should especially avoid projecting the project's takeover of market share or the token's future secondary market price.
- **Discussions of prior investments or major projects completed by the development team and its advisors or consultants:** In the *Munchee* Order, the SEC criticized statements highlighting "its founders had worked at prominent technology companies" and "their skills running businesses and creating software." This suggests a Token Sponsor should be cautious about discussing the management and entrepreneurial skills and records of those involved with its token project in the context of a token's future financial performance or in such a way that creates an expectation that their efforts will help the price of the relevant digital token appreciate.

CONCLUSION

Following these *Principles and Guidelines for Token Sponsors* provides no guarantee that a federal or state regulator will not take issue with the digital token issuance, sale, or other distribution. Rather, these principles and guidelines are intended to provide an overview to assist a Token Sponsor when thinking through critical issues related to its digital token issuance, sale and distribution. These *Principles and Guidelines for Token Sponsors* should be read in concert with the *Token Alliance's Principles and Guidelines for Token Trading Platforms*.

SECTION 2 - PRINCIPLES AND GUIDELINES FOR TOKEN TRADING PLATFORMS

This Section provides introductory principles and guidelines for entities that allow the trading of digital tokens on their platforms and for Token Sponsors seeking to have their tokens traded on such platforms. This Section only addresses platforms (collectively, "Token Trading Platforms")[84] through which market participants can convert virtual currency, fiat currency, or other digital tokens into other virtual currency, fiat currency, or other digital tokens that are not:

- Registered with the SEC pursuant to the Exchange Act as a "national securities exchange" or an "alternative trading system;" or
- Registered with the CFTC pursuant to the CEA as a "registered entity."

TOKEN TRADING PLATFORM

Any entity that hosts customer-oriented spot markets and is neither (a) registered with the SEC pursuant to the Exhange Act as a "national securities exchange" or an "alternative trading system" nor (b) registered with the CFTC pursuant to the CEA as a "registered entity".

Token Trading Platforms and other secondary markets for digital tokens play a critical role in the establishment of secure networks, enhance token utility, and promote the general adoption of cryptocurrency and blockchain technology. They provide an important mechanism for price discovery, which in turn allows systems that incentivize blockchain validation—such as proof of work—to function efficiently. They also expand opportunities for the general public (*e.g.*, the unbanked) to acquire and benefit from blockchain applications, and to purchase and sell tokens as their demands for particular token functionalities change and evolve and as new and improved tokens are developed.

84 These Principles and Guidelines assume that the Token Sponsor is independent of the Token Trading Platform. Although a Token Trading Platform may make a market in a token for which it is the Sponsor, this reduces the need for formal reviews and agreements.

But secondary markets may also create securities law-related concerns. In the words of SEC Chairman Jay Clayton, a secondary market is a "key hallmark" of securities and of securities offerings.[85] Facilitating the trading of digital tokens may subject a platform to regulation by the SEC or the CFTC if the tokens are found to be securities or CFTC Regulated Instruments. The uncertainty surrounding the application of "facts and circumstances" legal tests to new and evolving blockchain technology makes compliance with those regulatory definitions challenging.

Of course, responsible Token Trading Platforms should do more than merely avoid regulation by the SEC or the CFTC. They should voluntarily conduct business in a manner that protects token consumers, protects the integrity of secondary markets, and builds public confidence in the broader blockchain industry.

These broader concerns, although important, are beyond the scope of this chapter, as are the following non-exhaustive list of other legal and regulatory issues that Token Trading Platforms should address:

- cyber security;
- whether their activities constitute money transmission under the relevant federal and state statutes and regulations;
- privacy and data transfer issues for international users;
- AML/KYC and OFAC procedures, including transparency surrounding such procedures so that users understand why they must provide their information;
- reserving the right to remove users from the exchange;
- reserving the right not to conduct cross-chain recoveries when people deposit the wrong tokens in exchange wallets; and
- how the exchange will treat victims of external phishing schemes or theft of tokens.

Rather, this Section will focus on how Token Trading Platforms may manage the risk that a regulator or a court may contend that a digital token trading on the platform is a security or CFTC Regulated Instrument notwithstanding the Token Sponsor's claims to the contrary. This is an important threshold concern for any Token Trading Platform because allowing even one security or CFTC Regulated Instrument to trade on the platform would require the Token Trading Platform to registered with either the SEC or CFTC, respectively.

85 SEC *supra* note 49; CLAYTON *supra* note 45. [These citations refer to footnotes 49 and 45 in Understanding Digital Tokens: Market Overviews & Proposed Guidelines for Policymakers & Practitioners (July 2018).]

I. IMPORTANT CONSIDERATIONS FOR VETTING TOKENS FOR ACCEPTANCE ONTO A TOKEN TRADING PLATFORM

- ✓ Before it establishes a market for any digital token, a Token Trading Platform should examine the token to determine the risk that it might be deemed to be a security or CFTC Regulated Instrument and, consequently, that the Token Trading Platform might fall within the requirements of the Exchange Act or CEA. No token should be exempt from this examination. Digital tokens for which markets were established before a Token Trading Platform adopted written procedures as described below should be reviewed retroactively.

- ✓ The compliance officer or other senior managers of the Token Trading Platform should establish written procedures ("Procedures"), containing factors used to evaluate digital tokens for approval for trading on the platform, as well as standards for ongoing review of tokens to assess if they will no longer be permitted to trade. The Procedures should include:

    - a review the token's present utility, based on the Token Sponsor's white paper and other documents, information, or demonstrations provided by the Token Sponsor;

    - a review of promotional statements (and any subsequent disclaimers) made by the Token Sponsor or agents on its behalf on public-facing media;

    - a current written analysis prepared by the Token Sponsor's counsel or by the Token Sponsor in consultation with its counsel explaining why the digital token is not a security or CFTC Regulated Instrument, which analysis should be reviewed by counsel for the Token Trading Platform; and

    - a requirement that digital tokens are reviewed periodically to ensure that they remain compliant with existing law and regulatory expectations relevant to Exchange Act or CEA requirements.

- ✓ The same criteria should be used to close a market for a digital token as are used to deny a request to establish a market for a prospective token.

- ✓ A Token Trading Platform should memorialize the results of a token's examination and any re-examination and store them for no less than five years.

- ✓ A Token Trading Platform should not permit trading of any derivative instruments, including but not limited to any CFTC Regulated Instruments.

- ✓ A Token Trading Platform should carefully consider whether to permit trading of digital tokens on a leveraged, margined, or financed basis. If a Token Trading Platform were to permit trading of tokens in these ways, it should only do so where it has implemented appropriate measures to ensure such trading is in accordance with applicable CEA requirements.

- ✓ As illustrated by the *Munchee Order*, promises by a Token Sponsor to establish secondary trading markets for its digital token, or even publicized efforts by the Token Sponsor to do so, may be a

negative factor under the *Howey* Test. In light of this, a Token Trading Platform should consider its policies around (a) confidentiality of requests to establish a market and communications relating to such requests and (b) publicity regarding its decision to establish, to not establish, or to close a market for a digital token. The Token Trading Platform should take appropriate steps to inform applicants of and require applicants to abide by these policies.

- ✓ Adopt policies and procedures to ensure that a Token Trading Platform's directors, officers, employees, and affiliated third parties do not use nonpublic material information obtained through their work with the Token Trading Platform to engage in digital token transactions that could give the appearance of trading on material non-public information.[86]
- ✓ Have procedures for promptly investigating any reports of market manipulation.
- ✓ Establish criteria and procedures for suspending trading of a token suspected of being involved in manipulative trading activity.
- ✓ Involvement of a Token Trading Platform in the offering and distribution of a digital token may become a factor in determining whether a digital token qualifies as an investment contract under the *Howey* test. A Token Trading Platform may want to assess this risk with the Token Sponsor before becoming involved. Even after a market is established, a Token Trading Platform should avoid appearing to endorse as an investment any digital token that is trading on its platform and should make appropriate disclosures and disclaimers when necessary to counter any such appearance. This guidance is not meant to discourage communication between Token Sponsors and Token Trading Platforms for the purpose of clarifying or enhancing legal compliance or collaboration relating to technological issues associated with potential or continued inclusion of the digital token on the Token Trading Platform.

II. CONSIDERATIONS FOR TOKEN SPONSORS DEALING WITH TOKEN TRADING PLATFORMS

- » A Token Sponsor should keep in mind that no Token Trading Platform is obligated to maintain a market for its digital token and should be prepared to work with the Token Trading Platform to answer all reasonable questions that the Token Trading Platform asks of it.
- » A Token Sponsor should consider whether any financial dealings with a Token Trading Platform or its affiliates could create a reasonable impression that the Token Sponsor is "buying" the digital tokens' way onto the platform.
- » A Token Sponsor that deals with Token Trading Platforms should have policies and procedures to prevent its affiliates and employees from trading based on non-public information regarding the token's status on the platform, such as a decision to open or close a market for the token.

86 Sections 6(c) and 9(a) of the CEA, CFTC Regulation 180, and associated guidance and case law may be relevant to such policies and procedures.

- While a Token Sponsor may publicize that its token can be purchased or sold on a Token Trading Platform, once a market for the token is opened, the Token Sponsor should refrain from discussing the token's potential for price appreciation.

CONCLUSION

Following these *Principles and Guidelines for Token Trading Platforms* provides no guarantee that a federal or state regulator will not take issue with the trading of particular tokens on its Token Trading Platform. Rather, these principles and guidelines are intended to provide an overview to assist a Token Trading Platform when thinking through important considerations before establishing a market for digital tokens. These *Principles and Guidelines for Token Trading Platforms* should be read in concert with the *Token Alliance's Principles and Guidelines for Token Sponsors*.

V. APPENDIX

Whereas the information available in Chart 1 in the Introduction is condensed and provided as a means of comparison between the registration requirements and restrictions of certain types of offerings, the information below is intended to elaborate on the requirements and supplement the brief descriptions in the Chart.

I. SECURITIES TOKEN OFFERINGS

Pursuant to Section 5 of the Securities Act, any offer or sale of a security made to U.S. persons must either be (1) registered with the SEC or (2) offered and sold pursuant to an exemption from registration. Section 6 of the Securities Act, describes the method of registration and related considerations.

A. OFFERINGS REGISTERED WITH THE SEC UNDER SECTION 6 OF THE SECURITIES ACT

1. STRUCTURE

In order to register an offering of securities under Section 6, an issuer must file a registration statement with the SEC.[87] Pursuant to Section 10 of the Securities Act, the issuer must prepare a statutory prospectus to be delivered to prospective purchasers and integrated in the registration statement.[88]

Once the registration statement is filed, the SEC will review it, provide comments to the issuer and, if the statement is judged to be satisfactory, declare the registration statement effective.

2. MANNER OF SALE LIMITATIONS

Issuer requirements	There are no statutory limitations on the types of issuers that can undertake registered securities offerings. However, the Securities Act alleviates some of the regulatory burdens associated with registered offerings for certain well-known reporting issuers

87 U.S. domiciled issuers generally would file Form S-1, while foreign issuers would file Form F-1.
88 Securities offerings that are not registered and do not have an available exemption are prohibited pursuant to Section 5 of the Securities Act.

Investor requirements	There are no statutory restrictions on the type of investors that can participate in registered offerings
Limits on amounts raised	Issuers undertaking registered offerings are not subject to any regulatory offering limit within a 12-month period.
General solicitation	Before a registration statement is filed, often referred to as the "pre-filing period", oral or written offers for the sale of securities are generally prohibited. The SEC has stated that during the pre-filing period, "the publication of information and statements, and publicity efforts, made in advance of a proposed financing which have the effect of conditioning the public mind or arousing public interest in the issuer or in its securities constitutes a violation of the [Securities] Act." After an issuer files a registration statement, oral offers and certain written offers may be made pursuant to a statutory Section 10 prospectus, a Section 10 free writing prospectus and Rule 134 public notice (tombstone ad). However, until the registration statement becomes effective, there can be no sale of securities.
State law preemption	Only SEC-registered securities offerings that are listed on a national securities exchange are preempted from state registration requirements
Transferability of tokenized securities	Tokenized securities issued pursuant to a registered offering will be freely tradeable on registered exchanges or alternative trading systems ("ATS"), subject to complying with applicable exchange listing standards and meeting relevant ATS trading requirements.

3. RELATIVE COSTS AND BENEFITS

Registered offerings provide the most permissive structure with regard to manner of sale limitations, including the ability to sell tokenized securities to retail customers. However, the main drawbacks of this structure are: (i) Cost – An issuer in a registered offering is likely to incur costs in excess of $2 million; (ii) Time – The preparation of a registration statement along with the SEC review process is time consuming and can take longer than one year; (iii) Disclosure and Periodic Reporting – As part of the initial registration statement, issuers are required to include audited financial statements and will be required to continue public reporting on a quarterly basis.

4. EXAMPLES OF REGISTERED TOKENIZED SECURITY ISSUANCES

1. Overstock.com

2. Monster Products, Inc.

3. The Praetorian Group, Inc.

B. EXEMPT OFFERINGS

Given the high transaction costs associated with registered offerings and being a public company, issuers have increasingly relied on exemptions from registration, such as the ones discussed below.

1. PRIVATE PLACEMENTS GENERALLY

Section 4(a)(2) of the Securities Act exempts "transactions by an issuer not involving any public offering" from the Section 5 registration requirements. These transactions are commonly referred to as private placements. Pursuant to Section 4(a)(2), the SEC has promulgated Regulation D which provides a "safe harbor" rule for private placements (including Rule 506(b) and 506(c)).[89] While issuers are able to conduct private placements by relying solely on the Section 4(a)(2) statutory exemption, given the relative ambiguity of the statutory language and requirements[90] and the lack of state law preemption for statutory private placements, issuers typically structure their private placements to comply with Rule 506(b) or 506(c) under Regulation D.

a. Potential structures

Issuers relying solely on the Section 4(a)(2) statutory exemption need not file any documentation with the SEC but may need to produce disclosure documentation depending on the sophistication of the potential investors being targeted.

Issuers relying on Rule 506(b) or Rule 506(c) are required to file Form D[91] with the SEC within 15 days after the first sale of securities and provide different levels of disclosure information to investors depending on the sophistication of the potential investors being targeted.

b. Manner of sale limitations

Issuer requirements – There are no statutory limitations on the types of issuers that may conduct private placements in reliance of Section 4(a)(2). However, the Regulation D safe harbors are not available for any issuer if it or its affiliates, executives and certain

89 17 C.F.R. § 230.500 *et seq.*
90 It is important to note that issuer's intending on relying on an exemption from registration will have the burden of proving that they have perfected the exemption by establishing that they have satisfied the necessary conditions.
91 https://www.sec.gov/about/forms/formd.pdf.

other related persons, have been subject to certain enforcement actions (the "bad actor disqualifications").[92]

Investor requirements – Issuers undertaking a private placement in reliance on Section 4(a)(2) must ensure that all persons to whom offers are made have financial sophistication (or have access to financially sophisticated advisors) and have access to the type of information that would be contained in a registration statement.[93]

Issuers undertaking a private placement pursuant to 506(c), must take reasonable steps to verify that all purchasers are accredited investors.[94] Certain bad actors are disqualified from participating in Rule 506(c) offerings.

Issuers undertaking a private placement pursuant to 506(b) are able to offer and sell securities to as many as 35 sophisticated but non-accredited investors. The issuer, prior to the sale, must "reasonably believe" that each non-accredited investor has knowledge and experience in financial and business matters and that he or she is capable of evaluating the merits and risks of the prospective investment.

Amount raised – There is no monetary limit to the amount of funds that can be raised pursuant to Section 4(a)(2) or Regulation D.

General solicitation – Pursuant to Section 4(a)(2) and Regulation D, an issuer cannot engage in "any form of general solicitation or general advertising."[95] As indicated by the SEC in various No-Action Letters, in the context of Regulation D, issuers may avoid "general solicitation" by limiting offers to prospective investors with whom they have pre-existing relationships that allow the issuer to evaluate a prospective investor's financial sophistication. Private placements conducted under Rule 506(c), however, permit general solicitation.

State Law Preemption – As compared to private placements done in reliance of Section 4(a)(2) where there is no preemption of state law, private placements pursuant to Regulation D preempt the application of state laws (including registration and qualification). However, in either case, the states retain the authority to require notice filings and collect state fees.

Transferability of tokenized securities – Tokenized securities issued pursuant to a private placement will be considered "restricted securities" under the Securities Act and the issuer should take certain precautions against their resale.

---

92 17 C.F.R. § 230.262.

93 *See SEC v. Ralston Purina Co.*, 346 U.S. 199 (1953) at 124 (finding that the availability of the Section 4(a)(2) exemption turned on "whether the particular class of persons affected needs the protection of the [Securities] Act.").

94 Under Rule 501 "accredited investors" include certain institutional investors as well as individuals whose net worth, or joint net worth with a spouse, exceeds $1 million (not including the value of one's residence) and those who had an individual income exceeding $200,000 in each of the two most recent years (or $300,000 joint income with one's spouse) and who reasonably anticipate such an income for the current year.

95 17 C.F.R. § 502(c).

2. OFFERING PURSUANT TO REGULATION A UNDER THE SECURITIES ACT[96]

a. Potential Structures

Issuers intending to engage in a Regulation A offering will be required to submit Form 1-A for review by the SEC, which consists of three parts: Part 1 (Notification); Part 2 (Offering Circular); and Part 3 (Exhibits). The Offering Circular is fairly substantial and "akin to what is required for smaller reporting companies in a prospectus for a registered offering," including information about the issuer, risk factors, plan of distribution, use of proceeds, etc.[97] Offerings pursuant to Regulation A must comply with the requirements of either Tier 1 or Tier 2.[98] If issued pursuant to Tier 2, the issuer must file two years of audited financial statements, while Tier 1 issuers may file unaudited financial statements. Both Tier 1 and Tier 2 permit issuers to submit draft offering statements to the SEC for confidential review before filing. Offering statements must be "qualified" by means of a "notice of qualification" from the SEC before any sales may be made pursuant to Regulation A.

After a Tier 2 offering, an issuer becomes a "mini reporting company" that is required to furnish the SEC with annual and semi-annual reports, as well as current reports of significant events. Tier 1 issuers do not have continuing reporting obligations, other than the obligation to provide certain information on Form 1-Z within 30 days after the completion or termination of the offering. Tier 2 issuers provide similar information on either Form 1-K or Form 1-Z, depending on whether the offering is terminated or completed.

b. Manner of Sales Limitations

Issuer requirements – Regulation A offerings are limited to privately held companies domiciled and having their principal place of business in the United States or Canada.[99] Issuers can be barred from undertaking Regulation A offerings based on the presence of "bad actors." Issuers that are registered as investment companies under the Investment Company Act of 1940 may not conduct offerings under Regulation A. Regulation A is also not available for blank check companies nor special purpose acquisition companies. It also cannot be used by issuers that have a class of securities registered under the Exchange Act.

Investor requirements – Regulation A imposes no limits on the number of offerees or purchasers and offers and sales are generally open to both accredited and unaccredited investors. While Tier 1 Regulation A offerings have no statutory investor requirements,

96 17 C.F.R. §§ 230.251-263.
97 Amendments for Small and Additional Issues Exemptions under the Securities Act (Regulation A), Securities Act Release Nos. 33-9741; 34-74578; 39-2501 ,75 Fed. Reg. 21806 (Apr. 2015).
98 *See* Rule 251 of Regulation A, 17 C.F.R. § 230.251.
99 Recently enacted legislation requires the SEC to amend Regulation A to permit public companies to use Regulation A. *See, e.g.*, Regulation A+ Expansion, https://www.blockchainlawcenter.com/blog/blockchain-law-center/regulation-a-expansion.

Tier 2 offerings subject non-accredited investors to investment limits.[100]

Amount raised – Issuers undertaking a Tier 1 offering are subject to an offering limit of $20 million within a 12-month period. Issuers undertaking a Tier 2 offering are subject to an offering limit of $50 million within a 12-month period.[101]

General solicitation – For both Tier 1 and Tier 2 offerings, Regulation A authorizes general solicitation and the use of broker-dealers to advertise and distribute the securities. Prior to conducting a Regulation A offering, a prospective issuer may "test the waters" for potential investor interest, although special disclaimers for these communications are required by Rule 255 under the Securities Act.

State Law Preemption – If an issuer undertakes a Tier 1 Regulation A offering, state blue sky laws are not preempted. If an issuer undertakes a Tier 2 Regulation A offering, state blue sky laws regarding pre-offering review are preempted.

Transferability of tokenized securities – Securities issued pursuant to a Regulation A offering are freely transferable (i.e., they are not restricted securities).

c. Relative costs and benefits for tokenized securities offerings[102]

i. Benefits

1. Issuers gain the ability to sell tokenized securities to retail investors.

ii. Costs

1. This process is time consuming, expensive, and can take up to one year.
2. Audited Financial Statements – If structured as a Tier 2 offering, issuers must include audited financials in the offering statement and be subject to ongoing reporting obligations.

II. REGULATION CROWDFUNDING

A. POTENTIAL STRUCTURE

Section 4(a)(6) of the Securities Act exempts an issuer from the Section 5 registration requirements for crowdfunding transactions that meet the requirements outlined below. Issuers relying on Section 4(a)(6) are required to file Form C with the SEC prior to the commencement of the offering.

---

100 Unless the securities are listed on a national stock exchange upon qualification, the amount of Tier 2 securities that may be purchased by any single non-accredited investor in any year is limited to not more that (a) the greater of 10% of the investor's annual income or net worth, in the case of an individual investor or (b) the greater of 10% of the investors annual revenue or net assets, in the case of an entity.

101 "At the market" offerings are not permitted under Regulation A.

102 To date, the SEC has approved two token offerings under Regulation A. *See* Paul Vigna, *SEC Clears Blockstack to Hold First Regulated Token Offering*, WALL STREET JOURNAL (July 10, 2019), https://www.wsj.com/articles/sec-clears-blockstack-to-hold-first-regulated-token-offering-11562794848; *see also* Press Release, Props, Props Launches the First SEC-Approved Crypto Token for Consumers (July 11, 2019), https://www.businesswire.com/news/home/20190711005651/en/Props-Launches-SEC-Approved-Crypto-Token-Consumers.

Form C includes some basic information relating to the offering, including the name of the intermediary through which the tokenized securities will be offered, the compensation of the intermediary, the type and number of tokenized securities being offered, their price, and other information about the issuer. Form C is relatively simple when compared to Form 1-A, which is required for Regulation A offerings.

Issuers undertaking a Section 4(a)(6) offering must also provide a range of financial disclosure. Issuers offering tokenized securities in reliance of Regulation Crowdfunding for the first time must provide two years of financial statements reviewed by an independent public accountant. However, repeat issuers must provide two years of financial statements that are audited.[103] Issuers selling tokenized securities pursuant to the crowdfunding exemption are also required to file an annual report with the SEC no later than 120 days after the end of the fiscal year.

1. MANNER OF SALE LIMITATION

Issuer requirements – Excludes non-U.S., blank-check, reporting, and investment companies. "Bad actor" disqualifications apply.

Investor requirements – Sales are open to both accredited and unaccredited investors. Investment limitations are based on annual income and net worth.

- If either the annual income or the net worth of the investor is less than $100,000, the investor is limited to the greater of $2,000 or 5% of the lesser of his or her annual income or net worth.
- If the annual income and net worth of the investor are both greater than $100,000, the investor is limited to 10% of the lesser of his or her annual income or net worth, to a maximum of $100,000.

Limits on amounts raised – Issuers undertaking a Regulation CF offering are limited to raising $1.07 million over a 12-month period.

General solicitation – Issuers must undertake a Regulation CF offering exclusively through one intermediary that is registered as either a broker-dealer or a "funding portal," and that is also a member of a national securities association (e.g., FINRA).[104] Unlike Regulation A, issuers relying on Regulation CF are not permitted to "test the waters" to determine investor interest. However, after Form C is filed, issuers are permitted to engage in limited advertising. For example, issuers are permitted to communicate with potential investors through the intermediary's platform.

State Law Preemption – Tokenized securities issued pursuant to Regulation CF will not be subject to state blue sky laws.

Transferability – Tokenized securities issued pursuant to a Regulation CF offering cannot be transferred for 12 months after issuance.

103 80 Fed. Reg. 71, 387 (Nov. 16, 2015).
104 Portals like Indiegogo, which already had a crowdfunding portal, have recently launched token offerings.

TOKEN ALLIANCE

CHAMBER OF DIGITAL COMMERCE

UNDERSTANDING DIGITAL TOKENS

Consumer Protection Considerations and Guidelines

Prepared by the Token Alliance – an industry initiative of the Chamber of Digital Commerce

FIRST EDITION • AUGUST 2019

CONSUMER PROTECTION CONSIDERATIONS AND GUIDELINES

The Chamber of Digital Commerce would like to thank the following individuals and organizations for their valuable contributions to the Token Alliance in the production of this report.

We would also like to extend a special thank you to **Greg Strong of DLx Law LLP** and **Elizabeth McKeen of O'Melveny & Myers LLP** for helping to lead the development of this report.

THOMAS BORREL
Polymath

PAUL BRIGNER
Chamber of Digital Commerce

KENDRA HAAR
Perkins Coie LLP

OLGA MACK
Quantstamp

ELIZABETH MCKEEN
O'Melveny & Myers

DIVIJ PANDYA
Chamber of Digital Commerce

GREG STRONG
DLx Law LLP

COLLEEN SULLIVAN
CMT Digital

DAWN TALBOTT
RiskSpan

LILY WONG
Trust Token

TABLE OF CONTENTS

II. INTRODUCTION

This new installment of our series of reports is an important addition to the overall regulatory and market consideration of the token ecosystem. The way in which digital tokens operate is complex and can maintain multiple characteristics – from an investment contract, to something necessary for utilizing a digital platform, to a form of payment or exchange, to name just a few. We are in a moment when technological advancement is pushing the boundaries of decades-long established law – law that was made at a time when tokenized assets and instantaneous digital transfers of value were not contemplated. It is exciting to be a part of it, but it also entails risks.

To facilitate the development of token businesses as well as minimize incidents of fraud and compliance challenges, the Chamber embarked on a plan to tackle each of the issues impacting this ecosystem. This journey started with a publication of guidelines for digital tokens that were intended to operate outside Securities and Exchange Commission (SEC) and Commodity Futures Trading Commission (CFTC)-regulated products and services laws (so-called "utility tokens" and associated platforms).

Those Guidelines also sought to provide legal context by detailing the legal landscapes governing digital tokens in five countries – the United States, Canada, the United Kingdom, Australia, and Gibraltar. Taking up a sizeable portion of the Report, the description of the vast number of potential legal requirements and government oversight demonstrated that this is a regulated industry, no matter where you fall in the spectrum of token categorization.

Finally, we provided an economic perspective on the industry with an analysis of market trends. The sheer volume of capital raised demonstrates the passionate interest of so many around the world in the potential of these markets – whether as a way to make money, a way to use new and better services, or other reasons.

This installment expands on those initial resources to balance out the conversation around utility tokens to discuss the rules, regulations, and resulting considerations for those who wish to issue or trade tokens that are or otherwise represent securities. This sector of the market is growing with entrants from new technology companies as well as established institutional financial services providers. The securities laws are complex, generated in the 1930s and developing substantial legal and regulatory precedent. In some cases, that precedent has endured because it is principles-based. In others, it has become outdated as it no longer sufficiently contemplates the types of securities that can be created, issued, held, and traded digitally.

We are excited to introduce these guidelines for consumer protection related to digital tokens. This complements our recent work on securities and non-securities tokens. But we can't stop there. More areas need to be considered and addressed with thoughtful analysis. In the coming days and weeks, we also intend to publish guidelines around cyber security and anti-money laundering. We will be supplementing our legal landscape on a rolling basis with the introduction of additional countries and the laws that apply to digital tokens.

We hope you enjoy these publications and that they serve to help guide your analysis and views of the evolving digital token ecosystem. We look forward to sharing this series as we roll out these publications throughout the coming weeks!

A few words of caution:

THIS REPORT DOES NOT CONSTITUTE LEGAL ADVICE

- Specifically, nothing in this report should be construed as advice regarding the law of the United States or any other jurisdiction.
- This report's analysis of the criteria under which it is determined that tokens constitute securities or commodities do not constitute a restatement of law.
- This report, including its suggested guidelines, merely express the general views of the Token Alliance, and compliance with such guidelines cannot assure that the distribution or trading of tokens will fully comply with the laws discussed herein.
- These views are being offered for discussion purposes only, and they have not been sanctioned by the SEC, CFTC, or any other regulator or government agency.

CONSULT LEGAL COUNSEL BEFORE DISTRIBUTING OR HOSTING TRADES OF DIGITAL TOKENS

- Token Sponsors and associated parties seeking to generate or distribute a blockchain-based token should seek independent legal counsel with expertise in this area before proceeding with their project, particularly given the fast-paced nature of this industry and the quickly evolving legal landscape.
- Counsel can help consider the facts and circumstances surrounding particular issues within the contours of then-current regulatory and enforcement activity.
- This report does not attempt to address any individual case, and the thought leadership contained herein is not appropriate for use as a substitute for independent counsel.
- Further, the digital token market is rapidly shifting and therefore the cases and regulatory interpretations discussed in this report may be overtaken by future events.

The Token Alliance will continue to study the issues surrounding the appropriate regulation for tokens and it will offer additional insights, as appropriate, when new developments arise.

III. CONSIDERATIONS AND GUIDELINES FOR CONSUMER PROTECTION

Consumer protection laws may apply to digital tokens in certain circumstances. In this report, we identify those circumstances most likely to result in the application of consumer protection laws to activities involving digital tokens, describe the source and scope of federal and state consumer protection authority, and provide guidelines to help token sponsors and token trading platforms avoid running afoul of consumer protection laws.

Federal and state consumer protection laws may apply to activities involving digital tokens. At the federal level, the Federal Trade Commission ("FTC"), the Consumer Financial Protection Bureau ("CFPB"), and the Department of Justice ("DOJ") all have consumer protection authority. The FTC has the authority to enforce the Federal Trade Commission Act ("FTC Act") which prohibits unfair or deceptive acts or practices ("UDAP") in or affecting interstate commerce.[1] The CFPB has the authority to enforce the Consumer Financial Protection Act ("CFPA") which prohibits unfair, deceptive, or abusive acts and practices ("UDAAP") engaged in by any person offering or providing a consumer financial product or service.[2] The Civil Division of the DOJ has a Consumer Protection Branch that coordinates with the FTC, CFPB, and other federal agencies to enforce consumer protection statutes throughout the United States.[3]

At the state level, state Attorneys General ("AGs") have broad consumer protection authority to protect their citizens from unfair and deceptive acts and practices.[4] State money-transmission licensing laws have consumer protection aspects that may apply in the context of transmission activities involving digital tokens.[5] Additionally, the New York Department of Financial Services' virtual currency regulations contain a consumer protection component.[6] This section will examine each agency in more detail.

1 15 U.S.C. § 45(a).
2 12 U.S.C. §§ 5531, 5536(a)(1)(B). The CFPA is Title X of the Dodd-Frank Act (Pub. L. No. 111-203, Tit. X, § 1001-1100H, 124 Stat. 1376 (July 21, 2010)).
3 *See* 28 C.F.R. § 0.45(j) (setting forth the Consumer Protection Branch responsibility for litigation under principal federal consumer protection laws).
4 *See* Carolyn Carter, Consumer Protection in the States, a 50 State Evaluation of Unfair and Deceptive Practices Laws, 9, Nat'l Consumer Law Ctr. (Mar. 2018).
5 *See* The State of State Money Services Businesses Regulation and Supervision, 4, Conference of State Bank Supervisors (May 2016), https://www.csbs.org/sites/default/files/2017-11/State%20of%20State%20MSB%20Regulation%20and%20Supervision%202.pdf.
6 23 N.Y. Comp. Codes R. & Regs. tit. 23, § 200.19.

I. FEDERAL CONSUMER PROTECTION AUTHORITY

A. FEDERAL TRADE COMMISSION

The FTC has the authority to enforce the FTC Act, which prohibits unfair and deceptive acts or practices in or affecting commerce.[7] An act or practice that "causes or is likely to cause substantial injury to consumers which is not reasonably avoidable by consumers themselves and not outweighed by countervailing benefits to consumers or to competition" is unfair.[8] A consumer injury must be substantial, and not merely trivial or speculative, in order to trigger application of the FTC Act.[9] Typically, substantial injury involves financial harm, and in some cases health and safety risks can also constitute substantial injury.[10] Subjective types of harm are usually not enough to cause substantial injury.[11]

The injury must also not be outweighed by countervailing benefits to consumers. For example, if providing complex disclosures to consumers regarding a product would cause the price of the product to increase, the consumer benefit of a lower price would be weighed against the potential harm associated with the lack of disclosure and the net effect considered. Finally, the injury must not be reasonably avoidable by consumers. Most actions alleging violations of Section 5 of the FTC Act are brought to address seller behavior that impedes individual consumer choice and decision making.[12] An act or practice that unjustifiably interferes with the ability of consumers to make their own free and informed purchasing decisions will usually be unfair for purposes of the Act.[13]

Misrepresentations or deceptive omissions of material fact also constitute deceptive acts or practices prohibited by Section 5(a).[14] There are three elements of deception cases considered by the FTC: 1) a misrepresentation, omission, or practice that is likely to mislead the consumer, 2) the act or practice must be viewed through the lens of a reasonable consumer, and 3) the misrepresentation, omission, or practice must be material.[15] A misrepresentation requires a representation that is likely to mislead and is material to the reasonable consumer.[16] An omission of material information occurs when information necessary to prevent a claim, practice, or sale from being misleading is not disclosed.[17] Practices related to marketing and point of sale representations can also be deceptive practices if they are likely to mislead consumers. Situations in which inaccurate or incomplete information is provided to prospective consumers in marketing materials or at the point of sale may constitute deceptive practices. The act or practice must be viewed through the objective lens of the reasonable consumer.[18]

---

7 15 U.S.C. § 45(a).
8 15 U.S.C. § 45(n).
9 FTC Policy Statement on Unfairness, Fed. Trade Comm'n (Dec. 17, 1980), http://www.ftc.gov/bcp/policystmt/ad-unfair.htm.
10 *Id.*
11 *Id.*
12 *Id.*
13 *Id.*
14 *See* Complaint for Permanent Injunction and Other Equitable and Monetary Relief, Fed. Trade Comm'n v. Equiliv Investments, No. 2:2015 cv 04379, ¶ 29, (D.N.J. June 24, 2015).
15 FTC Policy Statement on Deception, Fed. Trade Comm'n (Oct. 14, 1983), https://www.ftc.gov/system/files/documents/public_statements/410531/831014deceptionstmt.pdf.
16 *Id.*
17 *Id.*
18 *Id.*

If an act or practice would be likely to mislead a reasonable consumer, it is deceptive.[19] A consumer interpretation of an allegedly misleading act or practice that is not reasonable, but subjective, is not enough to deem the act or practice deceptive.[20] Finally, the representation, omission, or practice must be material – meaning it must be related to information that is important to consumers in making consumer decisions.[21]

ELEMENTS OF DECEPTION PRACTICES

1

A MISREPRESENTATION, OMISSION, OR PRACTICE THAT IS LIKELY TO MISLEAD THE CONSUMER

2

THE ACT OR PRACTICE MUST BE VIEWED THROUGH THE LENS OF A REASONABLE CONSUMER, AND

3

THE MISREPRESENTATION, OMISSION, OR PRACTICE MUST BE MATERIAL

In or affecting commerce means "commerce among the several States or with foreign nations, or in any Territory of the United States or in the District of Columbia, or between any such Territory and another, or between any such Territory and any State or foreign nation, or between the District of Columbia and any State or Territory or foreign nation."[22]

1. AUTHORITY OVER TOKEN SPONSORS AND TOKEN TRADING PLATFORMS

The FTC has not yet used its authority under the FTC Act to pursue an action alleging violations with respect to initial or secondary sales of digital tokens. However, the agency has released several consumer advisories regarding virtual currencies[23] and filed several actions involving companies in the virtual currency industry alleging violations of the FTC Act. An action against Butterfly Labs alleged violations of Section 5(a) of the FTC Act for failure to deliver computers designed to mine virtual currency to consumers after they had paid for them.[24] The violations were based on misrepresentations or deceptive omissions of material facts in connection with the advertising, marketing, promotion, offer, or sale of products or services.[25] The matter was resolved with the entry of a Stipulated Final Order for Permanent Injunction and Monetary Judgment.[26]

19 *Id.*
20 *Id.*
21 *Id.*
22 15 U.S.C. § 44.
23 *See, e.g.*, What to Know About Cryptocurrency, Fed. Trade Comm'n (Oct. 2018), https://www.consumer.ftc.gov/articles/what-know-about-cryptocurrency.
24 Complaint for Permanent Injunction and Other Equitable Relief, Fed. Trade Comm'n v. BF LABS, INC., d/b/a Butterfly Labs, et. al, No. 4:14-cv-00815-BCW, (W.D.Mo 2015).
25 *Id.*
26 Stipulated Order for Permanent Injunction and Monetary Judgment, Fed. Trade Comm'n v. BF LABS, INC., d/b/a Butterfly Labs, et. al, No. 4:14-cv-00815-BCW, (W.D.Mo 2015).

An action against Equiliv, d/b/a Prized, also alleged violations of Section 5(a) of the FTC Act and violations of New Jersey state consumer protection laws in connection with a rewards app that implanted malware on users electronic devices that then used the computing power of those devices to mine bitcoin without notice or authorization.[27] One alleged violation was based on misrepresentations in connection with the advertising, marketing, and promotion of the Prized mobile application that were misleading and deceptive.[28] Another violation alleged unfair conduct in connection with infecting and taking control of consumers' mobile devices with malware because that conduct caused, or was likely to cause, substantial injury to consumers that they could not reasonably avoid and was not outweighed by countervailing benefits to consumers.[29] This action was also resolved with the entry of a Stipulated Order for Permanent Injunction and Monetary Judgment.[30]

Finally, an action against Bitcoin Funding Team and My7Network alleged violations of Section 5(a) of the FTC Act in connection with a multi-level marketing scheme promoted as an opportunity for consumers to generate income and accumulate wealth by purchasing and donating bitcoin to earlier "upline" participants and by recruiting others to do the same.[31] These chain referral schemes were alleged to be deceptive acts or practices in violation of Section 5(a) of the FTC Act in part because the scheme offered no products or services and income was derived solely through payments by later participants.[32] This action is pending in the Southern District of Florida as of June 3, 2019.

The FTC could in the future use its authority to address allegedly unfair or deceptive acts or practices that are potentially harmful to consumers in the context of the generation and distribution of digital tokens. Such an application of this authority would likely be limited to the sale or distribution of tokens that are not subject to an alternative regulatory scheme, such as the securities laws or the commodities laws. If the FTC were to bring such an action, it would likely be with respect to a digital token that it believes to be a consumer good and neither a security nor a commodity.

B. CONSUMER FINANCIAL PROTECTION BUREAU

The CFPB has authority pursuant to the CFPA to address unfair, deceptive, or abusive acts and practices ("UDAAP") with respect to financial products offered primarily for consumer use by "covered persons" as defined by CFPA.[33] To date, the CFPB has not pursued a case alleging a violation of the CFPA in the context of a transaction in digital tokens and thus far has declined to extend Regulation E, governing electronic fund transfers involving consumers and financial institutions, to

27 Complaint for Permanent Injunction and Other Equitable Relief, Fed. Trade Comm'n v. Equiliv Investments, No. 2:2015 cv 04379, (D.N.J. June 24, 2015).
28 *Id.*
29 *Id.*
30 Stipulated Order for Permanent Injunction and Monetary Judgment, Fed. Trade Comm'n v. Equiliv Investments, No. 2:2015 cv 04379, (D.N.J. June 24, 2015).
31 Complaint for Permanent Injunction and Other Equitable Relief, Fed. Trade Comm'n v. Thomas Dluca, et. al, No. 0:18-cv-60379-KMM, (S.D.Fla. Feb. 20, 2018).
32 *Id.*
33 *See* 12 U.S.C. §§ 5481, 5531 & 5536(a) (2010).

virtual currencies.[34] It has released several consumer advisories regarding virtual currencies and the newly created Office of Innovation has proposed a product sandbox, trial disclosure sandbox, and revisions to the no-action letter policy in attempts to facilitate innovation and engagement with entreprenuers.[35]

The scope of CFPB authority in this area is narrow. Several key restrictions limit the scope of potential CFPB enforcement actions pursuant to the CFPA in connection with transactions involving digital tokens. First, the UDAAP provisions of the CFPA only apply to financial products offered or provided for consumer use.[36] The definition of "financial product or service" contains a list of products that fall within the definition and which are subject to CFPB jurisdiction when offered to consumers.[37] Although the list is long, it is difficult to imagine how most of the products or services might apply in the context of digital tokens. One type of service on the list which might be applicable includes "engaging in deposit-taking activities, transmitting or exchanging funds, or otherwise acting as a custodian of funds or any financial instrument for use by or on behalf of a consumer."[38] "[T] ransmitting or exchanging funds" means receiving currency, monetary value, or payment instruments from a consumer for the purpose of exchanging or transmitting the same by any means, including transmission by wire, facsimile, electronic transfer, courier, the Internet, or through bill payment services or other businesses that facilitate third-party transfers within the United States or to or from the United States.[39]

Second, CFPB jurisdiction is limited to covered persons who are generally providers of consumer financial products or services.[40] The term "covered person" means— (A) any person that engages in offering or providing a consumer financial product or service; and (B) any affiliate of a person described in subparagraph (A) if such affiliate acts as a service provider to such person.[41] The term "service provider" means any person that provides a material service to a covered person in connection with the offering or provision by such covered person of a consumer financial product or service, including a person who— (i) participates in designing, operating, or maintaining the consumer financial product or service; or (ii) processes transactions relating to the consumer financial product or service (other than unknowingly or incidentally transmitting or processing financial data in a manner that such data is undifferentiated from other types of data of the same form as the person transmits or processes).[42] In addition to covered persons, any person who knowingly or recklessly

34 Electronic Fund Transfers (Regulation E), 81 Fed. Reg. 70,319 (Nov. 14, 2016).
35 *See* Innovation, Consumer Fin. Prot. Bureau, https://www.consumerfinance.gov/about-us/innovation/ (last visited June 3, 2019); *See also* CFPB Office of Innovation Proposes "Disclosure Sandbox" for Companies to Test New Ways to Inform Consumers, Consumer Fin. Prot. Bureau (Sep. 13, 2018), https://www.consumerfinance.gov/about-us/blog/bcfp-office-innovation-proposes-disclosure-sandbox-fintech-companies-test-new-ways-inform-consumers/.
36 12 U.S.C. § 5531(a).
37 12 U.S.C. § 5481(5) and (15).
38 12 U.S.C. § 5481(15)(A)(iv).
39 12 U.S.C. § 5481(29).
40 12 U.S.C. § 5531(a).
41 12 U.S.C. § 5481(6).
42 12 U.S.C. § 5481(26)(A).

provides substantial assistance to a covered person or service provider in violation of the provisions of Section 5531 shall be deemed to be in violation of that section to the same extent as the person to whom such assistance is provided.[43]

Third, persons registered with or regulated by the U.S. Securities and Exchange Commission ("SEC") or U.S. Commodity Futures Trading Commission ("CFTC") are explicitly excepted from CFPB jurisdiction as long as they are acting within the scope of their registered or regulated capacity.[44]

The standards for unfair and deceptive acts and practices in CFPA are informed by the standards for those terms in the FTC Act, which are discussed above.[45] Accordingly, there are significant similarities with respect to the conduct prohibited by both the FTC Act and CFPA.

In the CFPA, unfair is defined as: "an act or practice that causes or is likely to cause consumers substantial injury that is not reasonably avoidable and if the substantial injury is not outweighed by countervailing benefits to consumers or to competition."[46] The standard for unfairness here is almost identical to the standard for unfairness in the FTC Act. The same is true for deception, which constitutes an act that: 1) misleads or is likely to mislead consumers; 2) the consumer's interpretation is reasonable under the circumstances, and 3) the misleading act is material.[47]

The UDAAP also prohibits abusive acts or practices.[48] What constitutes an abusive act or practice is less clear because it is not covered in the FTC Act, but such a practice must be one that:

- materially interferes with the ability of a consumer to understand a term or condition of a consumer financial product or service; or
- takes advantage of –
  - a lack of understanding on the part of the consumer of the material risks, costs, or conditions of the product or service;
  - the inability of the consumer to protect the interests of the consumer in selecting or using a consumer financial product or service; or
  - the reasonable reliance by the consumer on a covered person to act in the interests of the consumer.[49]

"Abusive acts or practices may also be unfair or deceptive," but each is distinct and "governed by separate legal standards."[50] The CFPB is considering addressing the abusiveness standard in future

43 12 U.S.C. § 5536(a)(3).
44 12 U.S.C. §§ 5481(20) - 5481(21).
45 CFPB Bulletin 2013-07 Prohibition of Unfair, Deceptive, or Abusive Acts or Practices in the Collection of Consumer Debts, n.1, Consumer Fin. Prot. Bureau (July 10, 2013), https://files.consumerfinance.gov/f/201307_cfpb_bulletin_unfair-deceptive-abusive-practices.pdf.
46 12 U.S.C. § 5531(c).
47 CFPB Bulletin 2013-07, *supra* note 45, at 3.
48 12 U.S.C. § 5531(a).
49 12 U.S.C. § 5531(d).
50 CFPB Bulletin 2013-07, *supra* note 45, at 4.

rulemaking,[51] but it has only pursued an action alleging abusive practices alone in the rarest of circumstances – most actions to date alleging abusive practices have alleged either unfair or deceptive practices as well.[52]

As described in detail above, the scope of CFPB authority in this space is narrow. The CFPB is constrained to regulating consumer financial products offered by covered persons that are not otherwise regulated by the SEC or CFTC. Accordingly, for the CFPB to assert jurisdiction, it would have to be with respect to a digital token that is neither a security nor a commodity, that constitutes a financial product, and is offered to consumers.

C. DEPARTMENT OF JUSTICE

The Consumer Protection Branch of the Civil Division of the Department of Justice (the "CPB") plays a role in U.S. federal consumer protection statute enforcement as well. The CPB handles consumer protection case referrals from client agencies, either directly or in coordination with a local United States Attorney's Office.[53] The Civil Division is specifically assigned to handle consumer litigation arising under the FTC Act in certain circumstances.[54] The FTC is a client agency of the CPB and the CPB is responsible for civil and criminal actions brought under the FTC Act, which generally fall within three categories: 1) enforcement actions for civil penalties and injunctive relief based on violations of final orders issued by the FTC; 2) enforcement actions for civil penalties and injunctive relief based on violations of FTC trade regulation rules; and 3) prosecutions for criminal violations of the FTC Act, and for violations of district court orders obtained under the FTC Act.[55]

The DOJ also works closely with the CFPB as a partner agency. The CFPB and the DOJ coordinate with respect to investigations and proceedings involving federal consumer financial laws[56] and may choose to bring coordinated enforcement actions in federal district court when appropriate. Most of the coordination to date between the CFPB and the DOJ has involved the Civil Rights Division and coordinated actions to enforce fair lending laws such as the Equal Credit Opportunity Act.[57] Future coordination of investigations and enforcement between the CFPB and DOJ in the area of digital tokens is possible pursuant to these procedures.

II. STATE CONSUMER PROTECTION AUTHORITY

A. STATE ATTORNEYS GENERAL

State AGs typically have broad authority to protect consumers from unfair and deceptive acts and

51 *See* Kelly Cochran, Fall 2018 Rulemaking Agenda (Oct. 17, 2018), https://www.consumerfinance.gov/about-us/blog/fall-2018-rulemaking-agenda/.
52 Adam Levitin, CFPB "Abusive" Rulemaking?, Credit Slips (Oct. 17, 2018), https://www.creditslips.org/creditslips/2018/10/cfpb-abusive-rulemaking.html.
53 Consumer Prot. Branch, Dep't of Justice, Monograph (2014), https://www.justice.gov/civil/consumer-protection-branch-18.
54 28 C.F.R. § 0.45(j).
55 *Id.*
56 12 U.S.C. § 5564(d)(2)(B) and Memorandum of Understanding between the Consumer Financial Protection Bureau and the Department of Justice, Consumer Fin. Prot. Bureau (Jan. 20, 2012), https://s3.amazonaws.com/files.consumerfinance.gov/f/2012/01/CFPB-DOJ-MOU.pdf.
57 *See, e.g.* Complaint, Consumer Fed. Prot. Bureau v. Bancorpsouth Bank, No. 1:16cv118-GHD-DAS, (N.D.Miss 2016).

practices.[58] State consumer protection statutes generally apply to consumer transactions involving products or services. These statutes are typically principles-based rather than rules-based, allowing them to be flexible, adaptable, and applicable to address a wide range of alleged misconduct. For example, state consumer protection statutes prohibiting unfair or deceptive acts or practices have been used in coordinated enforcement actions by state AGs to address activities as diverse as off-label marketing of drugs,[59] unfair debt collection,[60] misrepresentations regarding diesel emissions,[61] and misrepresentations regarding credit ratings,[62] to name a few.

Given the sweeping use of consumer protection authority by state AGs, it is likely that there will be investigations or actions involving digital tokens in the future. There have been no such actions to date and the activity with respect to digital tokens has been limited to consumer advisories about virtual currency. State consumer protection laws may be applied to digital tokens when they fall within the statutory definition of a good, service, or merchandise and there is a consumer transaction in a digital token that is alleged to have been unfair or deceptive. Notably, many state statutes include commodities in the definition of merchandise.[63]

Certain states have the authority to use consumer protection statutes to address unfair or deceptive practices involving securities. For example, the Insurance and Financial Services Division of the Massachusetts Attorney General's Office routinely uses its consumer protection authority with respect to matters involving securities.[64] In certain circumstances, state AGs have also sought to address alleged misconduct involving securities by bringing both securities and consumer protection claims. For example, in a series of coordinated actions against rating agency Standard and Poor's ("S&P") for alleged misconduct in connection with its ratings of structured finance securities, certain state AGs alleged that S&P violated both consumer and securities laws.[65] Accordingly, issuers of security tokens should be mindful of the potential for investigations or enforcement actions brought pursuant to state consumer protection authority.

State AGs also have the authority to enforce certain provisions of the CFPA, including, most importantly, the UDAAP provision.[66] State AGs can take enforcement actions in federal court to enforce this provision whenever they believe that an unfair, deceptive, or abusive act or practice has

58 State statutes may differ slightly in terms of the scope of authority and the conduct subject to the statute and other nuanced ways. For example, some states may not explicitly have authority to address unfairness, only deception – *See* Carter, *supra* note 4 at 14.

59 *See* Press Release, 51 Attorneys Geneal Reach Consumer Protection Settlement with Boehringer Ingelheim Pharmaceuticals, Inc. Concerning Off-Label Promotion of Four Prescription Drugs, Delaware.Gov (Dec. 20, 2017), https://news.delaware.gov/2017/12/20/bipi/.

60 *See* Faisal Sheikh, State AG-CFPB Settlement with Chase Bank over Credit Card Collections, StateAG.Org, https://www.stateag.org/policy-areas/consumer-protection/consumer-protection-resources/2016/11/26/state-ag-cfpb-settlement-with-chase-bank-over-credit-card-collections (last visited June 3, 2019).

61 *See* Delaware Consumers to be Compensated under Settlements with Volkswagen over Emissions Fraud, Delaware News (June 28, 2016), https://news.delaware.gov/2016/06/28/vw/.

62 *See* Press Release, Justice Department and State Partners Secure Nearly $864 Million Settlement with Moody's Arising from Conduct in the Lead up to the Financial Crisis, Department of Justice (Jan. 13, 2017), https://www.justice.gov/opa/pr/justice-department-and-state-partners-secure-nearly-864-million-settlement-moody-s-arising.

63 *See*, *e.g.*, 12 Del.C. § 2511(6).

64 15 M.G.L. c. 93A, § 1 defines "trade" and "commerce" to include "… any security as defined in subparagraph (k) of section four hundred and one of chapter one hundred and ten A and any contract of sale of a commodity for future delivery, and any other article, commodity, or thing of value wherever situate, and shall include any trade or commerce directly or indirectly affecting the people of this commonwealth."

65 The Attorneys General of Indiana, Missouri, and South Carolina alleged violations of both consumer protection and securities laws in their respective complaints. Each of these states also released these claims in connection with the ultimate resolution of these cases (*see* Settlement Agreement, ¶¶ 11.j., 11.n., and 11.r. (Feb. 2, 2015), https://www.justice.gov/file/338701/download.

66 12 U.S.C. § 5552(a)(1).

occurred in connection with the offer of a consumer financial product or service.[67] State AG authority is equal in scope to CFPB authority in this regard,[68] and in some states the ability to enforce the UDAAP provision of the CFPA increases the scope of consumer protection authority beyond what is provided for in the state consumer protection statutes alone. This potentially gives certain state consumer protection regulators the ability to address conduct through enforcement of the CFPA for which there would not be an otherwise viable action at state law. State AGs have coordinated with the CFPB on several CFPA enforcement actions.[69] As discussed, above, the applicability of the CFPA with respect to digital tokens is very narrow – the CFPA only applies to covered persons, offering a financial product or service when that product or service is offered to consumers. In addition, and unlike the state law authority outlined above, persons regulated by the SEC or CFTC are excluded from the coverage of the CFPA (which, from a policy perspective, makes sense in order to avoid subjecting entities to overlapping and duplicative regulatory schemes). Accordingly, a UDAAP action pursuant to the CFPA with respect to a security token is unlikely, whether pursued by the CFPB or State AGs.

B. STATE BANKING AUTHORITIES

State banking regulators generally regulate money services businesses including money transmitters.[70] Money transmission under state law generally means "selling or issuing payment instruments, stored value, or receiving money or monetary value for transmission."[71] State regulatory requirements are focused on consumer protection issues, in addition to ensuring the safety and soundness of money transmitters and adherence to Bank Secrecy Act and anti-money laundering requirements.[72] State law generally requires money transmitters to be licensed, in part for the protection of consumers.[73]

If you are engaging in the issuance, sale, redemption, storage, or trading of a digital token that functions as a store of value or medium of exchange, you may need to be licensed as a money transmitter in the states in which you operate. An analysis of your business model, the payment flows associated with your business, and the flow of digital tokens associated with your business should be completed with respect to each state in which you operate. In addition, consultation with an attorney with respect to this analysis is recommended so that a determination can be made with respect to any licensure obligations that may exist.

While specific laws vary from state to state, money transmitter licensing regimes typically include requirements that are designed, at least in part, with a consumer protection focus.[74]

67 *Id.*
68 Pursuant to 12 U.S.C. § 5552(b), a state attorney general or state regulator must provide notice to the CFPB prior to initiating any action pursuant to 12 U.S.C. § 5552(a)(1).
69 *See, e.g.,* Bureau of Consumer Fin. Prot. and New York v. Sterling Jewelers Inc., No. 1:19-cv-00448 (S.D.N.Y. 2019)(jointly alleging violations of the CFPA in addition to New York state law violations alleged by the New York Attorney General).
70 *See* CSBS *supra* note 5.
71 Unif. Money Serv. Act of 2004, § 102(14) (Unif. Law Comm'n 2004).
72 Conference of State Bank Supervisors, *supra* note 70, at 4.
73 *Id.* at 5.
74 *Id.* at 7.

Surety Bonds — Nearly every state requires a surety bond and nearly every state's statute or regulations permit the regulator to adjust the amount of the bond required based on the applicant's perceived risk. The bond serves as a form of insurance that will help repay customers if a licensee's business fails or the licensee commits fraud. Bond amounts vary from state to state, and the Uniform Money Services Act, section 204(a) proposes a bond in the amount of $50,000 plus $10,000 per location with a maximum addition of $250,000.[75]

Permissible Investments — Many states require licensees to maintain permissible investments with a market value equal to or greater than the aggregate amount of outstanding payment instruments and stored value obligations.[76] State regulators generally have the authority to limit the types of investments that are considered permissible, except for cash and certificates of deposit.[77] Several states have taken the position that a company who offers cryptocurrency wallet services must hold the equivalent value in cash; the majority of states permit a company to hold value in like-kind assets. For instance, if a company is storing $1 million worth of bitcoin on behalf of customers, if the company has $1 million in bitcoin on hand, that should satisfy the permissible investment requirement. Permissible investments requirements are a means of safeguarding funds to protect consumers.

Financial History & Projections — States protect consumers by requiring applicants for money transmission licenses to submit audited financials for prior years.[78] This requirement may be particularly difficult for new companies entering the digital asset industry as they may have limited operating history. Until recently, very few accounting firms would audit a company's records that included cryptocurrencies and digital assets. States want to see a proven track record of a financially healthy business that anticipates financial health in the future when state residents are going to be depositing money with a licensee.

Background Checks — States also attempt to protect the consumers of the state by checking the background of the applicant and the control persons behind the applicant. Specifically, the state is looking for any criminal convictions, bankruptcies, and the personal financial health of the leaders of a business. Applicants for money transmission licenses are generally required to provide this type of information in their application.[79] In addition, the regulator will typically conduct an investigation into these issues in connection with the evaluation of an application, which may include an on-site examination.[80]

75 Uniform Law Commission, *supra* note 71, at §204(a).
76 *See id.*at § 701(a).
77 *Id.*
78 *See* Uniform Law Commission, *supra* note 71, at § 202(c)(6).
79 *See id.* at § 202.
80 *Id.* at § 205(a).

C. NEW YORK STATE BITLICENSE

1. REGULATED PERSONS AND ENTITIES

On June 24, 2015, the New York State Department of Financial Services ("NYDFS") began requiring that persons or entities engaged in certain activities involving virtual currency in New York or involving a New York resident obtain a business license referred to as a "BitLicense."[81] In September 2015, NYDFS issued its first BitLicense; since then, it has issued only sixteen more BitLicenses, for which NYDFS charges a $5,000 application fee.[82]

The BitLicense regime applies to business activities involving virtual currency, defined as "[a]ny type of digital unit that is used as a medium of exchange or a form of digitally stored value."[83] This includes centralized and decentralized virtual currencies, as well as virtual currency that can be mined.[84] The definition expressly excludes digital units that exist solely within an online game and cannot be redeemed for fiat currency or real-world goods and services.[85] It also excludes digital units associated with customer rewards programs, even if those units can be redeemed for real-world goods and services, so long as they cannot be converted to fiat currency.[86]

The BitLicense regime regulates a wide range of business activities, including: (i) transmitting virtual currency; (ii) storing, holding, or maintaining custody or control of virtual currency on behalf of others; (iii) buying and selling virtual currency as a business; (iv) performing exchange services for customers; and (v) controlling, administering, or issuing virtual currency.[87] The types of activities most likely to be subject to regulation are those that involve e-wallets, token trading platforms, payment-processors, dealers, and virtual currency ATMs. Merchants who accept virtual currency in exchange for goods or services, miners of virtual currency, and virtual currency software developers are unlikely to be subject to BitLicense regulation.

2. CONSUMER PROTECTION REQUIREMENTS

One of the principal aims of the BitLicense is to protect consumers in the burgeoning market for virtual currencies. The BitLicense accomplishes this through a variety of strategies.

First, the BitLicense requires that licensees make numerous disclosures to consumers, both before and after engaging in any transaction. For example, licensees must disclose in writing to new customers prior to any transaction "all material risks associated with its products, services, and activities and Virtual Currency generally."[88] The regulation specifies ten such risks that,

81 *See* BitLicense Frequently Asked Questions, N.Y.State Dep't of Fin. Serv., https://www.dfs.ny.gov/legal/regulations/bitlicense_reg_framework_faq.htm.
82 *See* Alex Kadochnikov, New York's BitLicense costs $5,000, Hypergrid Business (July 18, 2015), https://www.hypergridbusiness.com/2015/07/new-yorks-bitlicense-costs-5000/.
83 N.Y. Comp. Codes R. & Regs. tit. 23, § 200.2(p).
84 *See id.*
85 *See* N.Y. Comp. Codes R. & Regs. tit. 23, § 200.2(p)(1).
86 *See* N.Y. Comp. Codes R. & Regs. tit. 23, § 200.2(p)(2)-(3).
87 *See* N.Y. Comp. Codes R. & Regs. tit. 23, § 200.2(q).
88 N.Y. Comp. Codes R. & Regs. tit. 23, § 200.19(a)(1)-(10).

"at a minimum," must be discussed, including that virtual currencies are not legal tender, that transactions in virtual currency may be irreversible, and that virtual currencies are volatile.[89] Licensees must also disclose in writing to new customers prior to any transaction "all relevant terms and conditions."[90] The BitLicense specifies a minimum set of terms that must be disclosed, including customer liability for unauthorized transactions and the licensee's right to disclose information about the customer's account in certain circumstances.[91] Finally, at the time of each transaction, licensees must disclose in writing the terms of the transaction, including at least the amount of the transaction, the amount of any fee(s), the type and nature of the transaction, a warning that the transaction may not be undone, and "such other disclosures as are customarily given" in such transactions.[92] Notably, the BitLicense requires that these written disclosures be made in English, as well as in any other predominant language(s) spoken by the customers.[93]

Second, the BitLicense requires that all licensees establish and maintain written policies for resolving complaints.[94] A licensee must also disclose on its website and in any physical business locations the contact information for its complaint department and inform consumers that they may also bring their complaint to NYDFS.[95]

Third, to enhance licensees' paper trail, the BitLicense requires licensees to provide a detailed receipt to customers.[96] The receipt must specify the licensee's name and contact information, the type, value, date, and time of the transaction, the fee and exchange rate, and statements about the licensee's liability for non-delivery or delayed delivery and its refund policy.[97] The licensee must also be prepared to provide its receipt form to NYDFS upon request.[98]

Fourth, the BitLicense requires that licensees take "reasonable steps to detect and prevent fraud, including by establishing and maintaining a written anti-fraud policy."[99] The licensee's anti-fraud policy must include, at minimum, an identification and assessment of fraud-related risk areas, procedures and controls to protect against the identified risks, a description of the allocation of responsibility for monitoring risks, and procedures for the periodic evaluation and revision of the anti-fraud procedures, controls, and monitoring mechanisms.

Finally, the BitLicense regulates licensees' advertising and marketing efforts. For example, licensees must include in advertisements their name and the fact that they hold a BitLicense.[100] Licensees must also retain all advertising and marketing materials for seven years.[101]

89 *Id.*
90 N.Y. Comp. Codes R. & Regs. tit. 23, § 200.19(b)(1)-(7).
91 *Id.*
92 N.Y. Comp. Codes R. & Regs. tit. 23, § 200.19(c)(1)-(5).
93 N.Y. Comp. Codes R. & Regs. tit. 23, § 200.19(a)-(c).
94 N.Y. Comp. Codes R. & Regs. tit. 23, § 200.20(a)-(b).
95 *Id.*
96 N.Y. Comp. Codes R. & Regs. tit. 23, § 200.19(e)(1)-(7).
97 *Id.*
98 N.Y. Comp. Codes R. & Regs. tit. 23, § 200.19(f).
99 N.Y. Comp. Codes R. & Regs. tit. 23, § 200.19(g).
100 N.Y. Comp. Codes R. & Regs. tit. 23, § 200.18(a).
101 *Id.*

3. ADDITIONAL REQUIREMENTS

The BitLicense also requires licensees to establish and maintain certain additional programs to protect the licensee and its customers.

Cybersecurity Program. BitLicense requires licensees to have an effective cybersecurity program protecting its systems and customers' accounts, including a written cybersecurity policy addressing a wide range of concerns and a comprehensive audit function for the program.[102] Licensees must also designate a Chief Information Security Officer,[103] submit an annual report to NYDFS assessing the cybersecurity program,[104] and employ and train cybersecurity personnel.[105]

Anti-Money Laundering ("AML") Program. The BitLicense requires licensees to have an AML program based on annual risk assessments conducted by licensees and submitted to NYDFS.[106] It must include, at minimum, a system of internal controls, policies, and procedures to ensure compliance, and must designate a qualified individual to oversee compliance with the AML program, and provide ongoing training for employees.[107] Licensees must also maintain detailed records of all virtual currency transactions, and notify NYDFS within 24 hours of conducting any transaction in virtual currency valued at over $10,000 not subject to currency transaction reporting requirements under federal law.[108]

Business Continuity and Disaster Recovery ("BCDR") plan. Finally, the BitLicense requires that licensees have a BCDR plan that: (i) identifies documents, data, infrastructure, personnel, and competencies essential to the licensee's business; (ii) identifies personnel responsible for implementing the BCDR plan; (iii) includes a plan for communicating with necessary personnel during an emergency; (iv) includes back-up system maintenance procedures; (v) includes data back-up procedures; and (vi) identifies third parties necessary to continue operation.[109] This BCDR plan must be provided to employees and tested annually.[110]

102 N.Y. Comp. Codes R. & Regs. tit. 23, § 200.16(a)-(b), (e).
103 N.Y. Comp. Codes R. & Regs. tit. 23, § 200.16(c).
104 N.Y. Comp. Codes R. & Regs. tit. 23, § 200.16(d).
105 N.Y. Comp. Codes R. & Regs. tit. 23, § 200.16(g).
106 N.Y. Comp. Codes R. & Regs. tit. 23, § 200.15.
107 N.Y. Comp. Codes R. & Regs. tit. 23, § 200.15(c)(1)-(4).
108 N.Y. Comp. Codes R. & Regs. tit. 23, § 200.15(e)(1)-(2).
109 N.Y. Comp. Codes R. & Regs. tit. 23, § 200.17(a).
110 N.Y. Comp. Codes R. & Regs. tit. 23, § 200.17(b) & (e).

III. GUIDELINES

The consumer protection laws outlined above aim to prevent potential consumer harm or to remedy such harm. Digital token sponsors and trading platforms should consider conducting an internal risk evaluation to assess the risk of potential consumer harm associated with the digital token(s) they distribute or trade and evaluating the sufficiency of controls in place to mitigate any such harm. Given the broad scope of the consumer protection laws discussed, it is likely that most digital token sponsors will have some degree of risk in this space, but understanding the components of that risk and the controls in place may permit digital token sponsors and trading platforms to better manage that risk.

Below is a non-exhaustive list of factors to consider in connection with an assessment of risk.

- What is the marketing strategy for your token?
- How are you advertising and marketing the token?
- Are all advertisements, marketing materials, and other consumer-facing representations regarding the token reviewed for clarity, accuracy, and completeness?
- Are all advertisements, marketing materials, and other consumer-facing representations regarding the token worded in a way that prospective consumers can understand?
- How is the token priced?
- How will the token be sold?
- If there are salespersons involved in the process, does salesperson compensation avoid promoting improper sales practices?
- How complex is the token and the blockchain-based platform on which it operates?
- What are your target customer demographics?
- What role, if any, do third parties play in connection with the sale or distribution of tokens?
- What role, if any, do third parties play in connection with the operation of the platform?
- What steps have been taken to establish a compliance policy that includes consumer protection considerations?

» How is that policy enforced?

» How is compliance with the policy monitored, both internally and with respect to any third parties involved in the platform?

» What other steps have been taken with respect to regulatory compliance?

» Are there policies in place to effectively handle consumer complaints regarding the digital token or the operation of the platform?

Conducting an internal risk assessment will help in following the below general guidelines.

» Avoid activity that might be viewed as unfair or deceptive in connection with the sale of digital assets.

- Ensure that all advertising, representations to consumers, and legal documents clearly, accurately, and fully describe all of the facts material to the prospective purchase of the digital assets being sold.
- Adhere to the policies and procedures (and marketing promises) you set out in all advertising, representations to consumers, and legal documents (do what you say you do).

» Token trading platforms should endeavor to avoid unfair, deceptive, or abusive acts or practices.

- Ensure that all advertising, representations to consumers, and legal documents accurately and fully describe all of the facts material to the prospective purchase of the digital assets being sold.
- Avoid any representations that might materially interfere with a consumer's ability to understand a financial product or service (abusive acts or practices).

» Entities engaged in Virtual Currency Business Activity involving New York or a New York resident will need to be licensed and comply with the consumer protection (as well as other) provisions of the BitLicense law.

TOKEN ALLIANCE

CHAMBER OF DIGITAL COMMERCE

UNDERSTANDING DIGITAL TOKENS

Guidelines for Anti-Money Laundering Compliance and Combatting the Financing of Terrorism

Prepared by the Token Alliance – an industry initiative of the Chamber of Digital Commerce

SECOND EDITION • SEPTEMBER 2019

GUIDELINES FOR ANTI-MONEY LAUNDERING COMPLIANCE AND COMBATTING THE FINANCING OF TERRORISM

The Chamber of Digital Commerce would like to extend a special thank you to the following individuals for helping to lead the development of this report.

SAM BORO
Perkins Coie LLP

STEVE BUNNELL
O'Melveny & Myers LLP

CHRIS CHRYSTAL
Perkins Coie LLP

KEVIN FELDIS
Perkins Coie LLP

KENDRA HAAR
Perkins Coie LLP

STEVEN MERRIMAN
Perkins Coie LLP

LAUREL LOOMIS RIMON
O'Melveny and Myers LLP

MICHAEL SELIG
Perkins Coie LLP

We would also like to thank the following individuals for their valuable contributions to the Token Alliance in the production of this report.

THOMAS BORREL
Polymath

PAUL BRIGNER
Chamber of Digital Commerce

GREG FAVITTA
CipherTrace

MICHELLE GITLITZ
Blank Rome

PHILLIP GRIFFIN
Wells Fargo

JOHN JEFFERIES
CipherTrace

OLGA MACK
Quantstamp

MICHAEL OU
CoolBitX Technology

DIVIJ PANDYA
Chamber of Digital Commerce

ARABY PATCH
Securitize

STEVEN SPRAGUE
Rivetz

DAWN TALBOTT
RiskSpan

SAM WYNER
KPMG

TABLE OF CONTENTS

II. INTRODUCTION

This new installment of our series of reports is an important addition to the overall regulatory and market consideration of the token ecosystem. The way in which digital tokens operate is complex and can maintain multiple characteristics — from an investment contract, to something necessary for utilizing a digital platform, to a form of payment or exchange, to name just a few. We are in a moment when technological advancement is pushing the boundaries of decades-long established law — law that was made at a time when tokenized assets and instantaneous digital transfers of value were not contemplated. It is exciting to be a part of it, but it also entails risks.

To facilitate the development of token businesses as well as minimize incidents of fraud and compliance challenges, the Chamber embarked on a plan to tackle each of the issues impacting this ecosystem. This journey started with a publication of guidelines for digital tokens that were intended to operate outside Securities and Exchange Commission (SEC) and Commodity Futures Trading Commission (CFTC)-regulated products and services laws (so-called "utility tokens" and associated platforms). Those Guidelines also sought to provide legal context by detailing the legal landscapes governing digital tokens in five countries — the United States, Canada, the United Kingdom, Australia, and Gibraltar. Taking up a sizeable portion of the Report, the description of the vast number of potential legal requirements and government oversight demonstrated that this is a regulated industry, no matter where you fall in the spectrum of token categorization.

Finally, we provided an economic perspective on the industry with an analysis of market trends. The sheer volume of capital raised demonstrates the passionate interest of so many around the world in the potential of these markets – whether as a way to make money, a way to use new and better services, or other reasons. This installment expands on those initial resources to balance out the conversation around utility tokens to discuss the rules, regulations, and resulting considerations for those who wish to issue or trade tokens that are or otherwise represent securities. This sector of the market is growing with entrants from new technology companies as well as established institutional financial services providers. The securities laws are complex, generated in the 1930s and developing substantial legal and regulatory precedent. In some cases, that precedent has endured because it is principles-based. In others, it has become outdated as it no longer sufficiently contemplates the types of securities that can be created, issued, held, and traded digitally.

We are excited to introduce these guidelines for anti-money laundering compliance to complement our work involving tokens. They supplement our reports on securities and non-securities tokens as well as consumer protection. AML compliance has always been a focus of industry from even before the time that FinCEN published its original guidance on convertible virtual currencies in 2013 and continues to be

a primary focus today. The latest approval by the FATF of Recommendations involving virtual assets and virtual asset service providers and FinCEN's most recent guidance for virtual currency businesses keep these issues at the forefront. We look forward to serving as a resource on this issue as technology, and criminal creativity, evolves.

We hope you enjoy these publications and that they serve to help guide your analysis and views of the evolving digital token ecosystem. We look forward to sharing this series as we roll out these publications throughout the coming weeks!

A few words of caution:

THIS REPORT DOES NOT CONSTITUTE LEGAL ADVICE

- Specifically, nothing in this report should be construed as advice regarding the law of the United States or any other jurisdiction.
- This report, including its suggested guidelines, merely express the general views of the Token Alliance, and compliance with such guidelines cannot assure that activities involving tokens will fully comply with the laws discussed herein.
- These views are being offered for discussion purposes only, and they have not been sanctioned by any regulator or government agency.

CONSULT LEGAL COUNSEL BEFORE ENGAGING IN ACTIVITIES INVOLVING DIGITAL TOKENS

- Token Sponsors and associated parties seeking to generate or distribute a blockchain-based token, as well as companies engaging in holding or transferring digital tokens on behalf of others should seek independent legal counsel with expertise in this area before proceeding with their project, particularly given the fast-paced nature of this industry and the quickly evolving legal landscape.
- Counsel can help consider the facts and circumstances surrounding particular issues within the contours of then-current regulatory and enforcement activity.
- This report does not attempt to address any individual case, and the thought leadership contained herein is not appropriate for use as a substitute for independent counsel.
- Further, the digital token market is rapidly shifting and therefore the cases and regulatory interpretations discussed in this report may be overtaken by future events.

The Token Alliance will continue to study the issues surrounding the appropriate regulation for tokens and it will offer additional insights, as appropriate, when new developments arise.

III. CONSIDERATIONS AND GUIDELINES FOR ANTI-MONEY LAUNDERING COMPLIANCE

I. INTRODUCTION

This report provides an overview of laws in the United States aimed at the prevention of money laundering and at combatting the financing of terrorists ("CFT"), as well as the rules and regulations that certain categories of businesses must follow with respect to establishing formal anti-money laundering ("AML") policies and practices. It concludes with a set of guidelines for token sponsors and token trading platforms to consider when crafting AML and CFT compliance programs.

II. CRIMINAL AND CIVIL ANTI-MONEY LAUNDERING LAWS

A. CRIMINAL ANTI-MONEY LAUNDERING LAWS

Any person or business conducting a financial transaction that occurs wholly or partially in the United States is obligated under the criminal laws[1] of the United States to avoid transacting in criminal proceeds. The term "financial transaction" under these statutes is expansive, including transactions as varied as money transfers, currency exchange, loans, use of a safe deposit box, or gifts of tangible property.[2] The following types of financial transactions are subject to criminal prosecution:

- *Concealment or Promotion of Money Laundering,* 18 U.S.C. § 1956(a)(1): This statute prohibits a transaction in which a person knows that the property involved in a transaction constitutes the proceeds of some form of unlawful activity, even if that person does not know the precise nature of the underlying criminal activity.[3] To be in violation of this law, there must be an intent on the part of the person conducting the transaction — most often proven through circumstantial evidence — to conceal the true nature, location, source, ownership, or control of the funds, or to reinvest in or "promote" future criminal activity.
- *International Money Laundering,* 18 U.S.C. § 1956(a)(2): This law applies even to "clean" funds that are not currently the proceeds of criminal activity but are sent to or from the United States to "promote" certain categories of criminal activity.

1 A civil suit seeking a monetary penalty may also be brought for violations of 18 U.S.C. § 1956 pursuant to subsection (b).
2 18 U.S.C. § 1956(c)(3) and (4).
3 The property involved must, in fact, be the proceeds of one of a number of "specified unlawful activities" — a broad category including most profit-generating crimes.

- *Money Spending Statute,* 18 U.S.C. § 1957: This law prohibits transactions over $10,000 where the participant[4] knows the funds are derived from some unlawful source.[5]
- *Money Laundering Conspiracy,* 18 U.S.C. § 1956(h): Two or more individuals who intend to conduct a transaction in criminal proceeds may be liable for any foreseeable offenses committed by their co-conspirators in furtherance of the scheme.

For those individuals or businesses who are engaged in activity that may be considered money transmitting, another criminal statute, 18 U.S.C. § 1960, makes it unlawful to operate a money transmitting business without a state license if operating in a state where one is required, or without registering as a "money services business" with the Financial Crimes Enforcement Network ("FinCEN"). Additionally, section 1960 makes it a crime for a money transmitting business to transmit funds that are known to be criminal proceeds or intended to promote certain types of criminal activity. Importantly, a violation of this statute can occur even where the operators of the business did not know a state license was required.[6] Additionally, criminal liability under this statute applies broadly to anyone who knowingly "conducts, controls, manages, supervises, directs, or owns all or a part" of such an unlicensed money transmitting business.[7]

B. CIVIL ANTI-MONEY LAUNDERING LAWS

Although every business that conducts financial transactions should be aware of criminal AML statutes, certain types of businesses are subject to a broad range of AML requirements under the regulatory regime established by the Bank Secrecy Act ("BSA"), 31 U.S.C. § 5311 *et. seq*. The BSA applies to a variety of "financial institutions," which include banks, credit unions, securities broker-dealers, currency exchangers, check cashers, issuers, redeemers or cashiers of travelers checks, and money transmitters, among other entities.[8] As discussed more fully below, for financial institutions subject to its jurisdiction, the BSA establishes various recordkeeping requirements as well as reporting requirements related to transactions in currency and monetary instruments. Additionally, the BSA mandates that financial institutions provide timely and detailed reports to law enforcement of suspicious transactions that occur within a business's purview. Parties (individuals or businesses) that willfully violate the BSA are subject to criminal penalties.[9]

III. ECONOMIC SANCTIONS

U.S. persons must comply with U.S. sanctions law. The U.S. government uses economic sanctions to advance its foreign policy and national security goals. Various U.S. statutes and Executive Orders authorize the imposition of these sanctions. The Department of the Treasury's Office of Foreign Assets Control ("OFAC") has primary responsibility for administering sanctions programs. OFAC, in total,

4 The statute is applicable to transactions conducted by "financial institutions," which includes, among other things, a currency exchange, money transmitter, and a broker or dealer in securities or commodities. 18 U.S.C. § 1956(c)(6); 31 U.S.C. § 5312(a)(2).
5 Again, the funds must actually be derived from a "specified unlawful activity;" even if the person involved is not aware of which particular unlawful activity.
6 18 U.S.C. § 1960(b)(1)(A).
7 18 U.S.C. § 1960(a).
8 31 U.S.C. § 5312(a)(1)(2).
9 31 U.S.C. § 5322.

administers over two dozen active sanctions programs for two categories of sanctions. First, OFAC administers targeted sanctions against specific individuals and entities and, in some cases, specific vessels and aircraft. OFAC maintains a Specially Designated Nationals and Blocked Persons List ("SDN List") that identifies the specific individuals, entities, and properties subject to sanctions as well as other sanctions lists. Second, OFAC administers comprehensive sanctions programs against entire countries or regions. Currently, OFAC has comprehensive sanctions in place against Cuba, Iran, North Korea, Syria, and the Crimea region of Ukraine.

WHO IS COVERED

U.S. persons must comply with sanctions regulations, although the definition of U.S. persons varies by sanctions program. In general, the sanctions programs cover:

- Any person within the United States;
- U.S. citizens (including citizens living abroad);
- Legal permanent residents of the United States;
- U.S. companies; and
- Foreign branches of U.S. companies.

Some sanctions programs go farther and cover foreign entities "owned or controlled" by U.S. persons. But even if the specific program does not cover such entities (and, thus, the entity itself is outside the scope of the sanctions program), a U.S. entity controlling a foreign entity would still be obligated to comply with U.S. sanctions.

U.S. persons are generally prohibited from transacting directly with a Specifically Designated National ("SDN") or a party residing in a sanctioned region (collectively, a "blocked party"). Even if a specific entity is not on the SDN list, U.S. persons may still be prohibited from transacting with the entity if SDNs, in the aggregate, own 50% or more of the entity. Likewise, U.S. persons are generally prohibited from conducting a transaction that involves property in which a blocked party has an interest. If a U.S. person determines that it is holding a blocked party's property, the U.S. person must block further transactions and, within 10 days of the blocking, file a blocked property report with OFAC.

FACILITATION

Even if a U.S. person does not transact directly with a blocked party, U.S. persons also violate sanctions laws if they approve or facilitate a transaction that would be prohibited if U.S. persons conducted the transaction directly. For instance, a U.S. citizen controlling a foreign entity may violate U.S. sanctions laws if the U.S. citizen authorizes the company to conduct a transaction with a blocked party. Similarly, U.S. persons cannot engage in a transaction that evades the prohibitions within a particular sanctions program.

STRICT LIABILITY

Assignment of fault and potential penalties for violating OFAC's sanctions regulations follow a standard of "strict liability." That is, the sanctions regulations do not incorporate an intent or a knowledge component. If a U.S. person engaged in a prohibited transaction (or facilitated a prohibited transaction), a sanctions violation can occur even where the violation was unintentional, unknown, or did not result from negligence.

PENALTIES

U.S. persons should take great care to avoid sanctions violations because the penalties can be severe. Some sanctions programs carry civil penalties that can be greater than $250,000 per violation or twice the amount of the violating transaction. Criminal penalties also can apply for willful sanctions violations.

VIRTUAL CURRENCIES

OFAC has made clear, through a series of FAQs, that the compliance obligations are the same whether the transaction is in fiat dollars or virtual currency. OFAC expects that virtual currency businesses subject to OFAC's jurisdiction will develop compliance programs tailored to each business's individual risks and designed to prevent transactions involving blocked parties and property.

THE VENEZUELAN PETRO

Still, there are sanctions compliance wrinkles unique to virtual currency businesses. U.S. persons are prohibited from engaging in transactions that relate to Venezuela's Petro, a virtual currency issued by the Venezuelan government. On March 19, 2018, President Trump signed Executive Order 13827 prohibiting U.S. persons from providing financing for or dealing in any "digital currency, digital coin, or digital token" that was "issued by, for, or on behalf" of the Venezuelan government.

WALLET ADDRESSES

On November 28, 2018, OFAC announced that it was adding two virtual currency addresses to the SDN List of two SDNs. OFAC's addition of virtual currency addresses to the SDN List means that, in addition to using traditional identifiers to screen out blocked parties and property, virtual currency businesses must also screen for and block transactions that involve blockchain addresses identified by OFAC as being associated with SDNs.

IV. REGULATION AND ENFORCEMENT ON THE FEDERAL AND STATE LEVEL

A number of different agencies on both the federal and state level exercise AML rule making, oversight, and enforcement authority over businesses subject to their jurisdiction. Because of this, a digital currency business may be subject to the simultaneous jurisdiction of multiple state and federal authorities, depending on the nature of their activities. Although federal regulators are primarily focused on compliance with the BSA and utilize a mostly consistent body of rules and agency guidance across agencies, state regulators' primary focus is different. On the state level, regulation and enforcement arises out of a focus on consumer protection and, although state regulators do generally require and

examine a licensee's BSA/AML programs, state licensing regimes are aimed primarily at ensuring safety and soundness of the financial institution to ensure consumer protection.

A. FEDERAL

A number of different agencies on the federal level are responsible for monitoring and enforcing laws and regulations targeting money laundering and terrorist financing. Regulatory agencies conduct regular and routine examinations of the activities of financial institutions and may bring civil enforcement actions assessing monetary penalties either independent of, or concurrent with, criminal enforcement actions.

1. FINANCIAL CRIMES ENFORCEMENT NETWORK

FinCEN is an agency within the U.S. Department of Treasury's Office of Terrorism and Financial Intelligence whose mission is to "safeguard the financial system from illicit use, combat money laundering, and promote national security through the strategic use of financial authorities and the collection, analysis, and dissemination of financial intelligence."[10] Although FinCEN has responsibility for ensuring businesses subject to its jurisdiction are in compliance with the BSA, it does not itself conduct examinations of those businesses.[11] Instead, examination authority for BSA compliance has been delegated to a number of other federal agencies and self-regulatory organizations. For example, depository institutions are examined by their own federal functional regulators (the Federal Reserve, the Federal Deposit Insurance Corporation, the Office of the Comptroller of the Currency, etc.); securities broker-dealers are examined by the Securities and Exchange Commission ("SEC") and the Financial Industry Regulatory Authority ("FINRA"); and money services businesses are examined by the Internal Revenue Service ("IRS"). Nonetheless, relying upon the findings of an examination or other sources of investigation, FinCEN has independent authority to bring civil enforcement actions, including monetary penalties and other injunctive relief.

2. SECURITIES AND EXCHANGE COMMISSION AND FINANCIAL INDUSTRY REGULATORY AUTHORITY

Broker-dealers and other participants in the market for securities are regulated by the SEC and are subject to compliance with the BSA and its implementing regulations.[12] Additionally, FINRA, a non-governmental self-regulatory organization that operates under the SEC's oversight, develops and enforces AML rules that apply to the activities of all registered broker-dealer firms and registered brokers in the United States. Both the SEC and FINRA conduct regular examinations of the entities within their jurisdiction, and, in the last year, both have announced exam priorities focused on AML programs.[13] Both agencies also have the authority to bring civil enforcement actions related to AML failures, which have included both corporate and individual penalties.

10 Fin. Crimes Enf't Network, Mission, https://www.fincen.gov/about/mission (last visited Aug. 15, 2019).
11 Govt. Accountability Office, *Anti-Money Laundering: U.S. Effort to Combat Narcotics-Related Money Laundering in the Western Hemisphere,* (Aug. 2017), https://www.gao.gov/assets/690/686727.pdf.
12 *See* Sec. 17(a) of the Securities Exchange Act of 1934, Rule 17a-8.
13 Office of Compliance Inspections and Examinations, 2018 National Exam Program Examination Priorities, Sec. and Exchange Comm'n (Feb. 7, 2018), sec.gov/about/offices/ocie/national-examination-program-priorities-2018.pdf.

3. COMMODITY FUTURES TRADING COMMISSION

The Commodity Futures Trading Commission ("CFTC") oversees individuals and organizations participating in derivatives markets and other products subject to the Commodity Exchange Act, including, among other things, swap execution facilities, derivatives clearing organizations, swap dealers, futures commission merchants, and commodity pool operators. The AML program requirements contained in the BSA and its regulations apply to futures commission merchants and introducing brokers regulated by the CFTC. The CFTC relies on the National Futures Association ("NFA"), the self-regulatory organization for the derivatives industry that it oversees, to establish and enforce rules implementing AML requirements for the NFA's registered members. The NFA conducts routine examinations of its members and brings enforcement actions that may include civil monetary penalties for violations of AML compliance rules.[14]

4. DEPARTMENT OF JUSTICE

The Department of Justice ("DOJ") has authority to investigate and prosecute criminal and civil enforcement actions related to violations of federal AML and CFT laws. Working with a number of federal investigatory agencies, including the Federal Bureau of Investigation, IRS, Drug Enforcement Administration, Homeland Security Investigation, and others, the DOJ conducts grand jury investigations and brings criminal and civil prosecutions of individuals and businesses under federal money laundering, money transmitting, and terrorist financing laws. Because money laundering is a criminal offense under various federal statutes, the DOJ's prosecutions can include and have included actions against financial institutions — and their compliance officers and executives — for violations of laws prohibiting money laundering and terrorist financing.[15] A prosecution may be brought by one of the 94 U.S. Attorney's Offices located throughout the country, or by an office within the DOJ headquarters in Washington, D.C., typically DOJ's Money Laundering and Asset Recovery Section ("MLARS"),[16] or jointly by both offices.

Unlike civil regulators that are charged with ensuring regulated entities maintain appropriate and effective AML programs, the DOJ is focused on prosecuting those entities and individuals who engage in or facilitate criminal money laundering or terrorist financing — including turning a blind eye to such activity taking place. The DOJ has a long history of pursuing criminal sanctions — imprisonment, fines, and forfeiture — against individuals and companies violating federal AML and CFT laws.

B. STATE

On the state level, financial activity affecting state residents is subject to oversight by both a state's financial regulators, a state's Attorney General, and other local law enforcement agencies.

---

14 Complaint, In the Matter of LBS Limited Partnership (NFA ID #245169), Nat'l Futures Ass'n (June 11, 2018), https://www.nfa.futures.org/basicnet/CaseDocument.aspx?seqnum=4558.

15 *See, e.g.,* DOJ, Banamex USA Non-Prosecution Agreement, Attachment A at 1 (May 18, 2017) (finding BSA violation where MSB failed to "provide appropriate staffing and resources to ensure its BSA department could conduct appropriate transaction monitoring").; *In the Matter of Ripple Labs* (DOJ May 5, 2018).

16 Dept. of Justice, *Money Laundering and Asset Recovery Section* (MLARS), https://www.justice.gov/criminal-mlars (last visited Oct. 19, 2018).

1. FINANCIAL REGULATORS

Almost all states in the United States regulate the transmission of money, and many states have robust licensing programs that require businesses to be licensed for that activity before engaging in any transactions with residents of a particular state. Across the United States, licensing regimes commonly include a registration requirement, the collection of biometric information for executives and other persons in "control," a surety bond, minimum capitalization requirements, and submission to regular state regulator examinations.[17] The onerousness of these requirements varies by state, as does the specificity of the agency guidance that can assist companies with navigating the requirements. Many states participate in the Conference of State Bank Supervisors ("CSBS"), a consortium of state banking regulators. CSBS oversees the National Multistate Licensing System ("NMLS"), which states increasingly use to process applications for money transmitter licenses.[18] CSBS also issues policies and reports that may influence state regulator action. The CSBS issued a model regulatory framework on September 15, 2015, that was designed to support the CSBS Policy on State Regulation of Virtual Currency and to promote consistent state regulation of virtual currency activities.[19]

In February 2018, seven states committed to a multi-state agreement ("Multistate Compact") that standardizes key elements of the licensing process for money services businesses.[20] For startups in the fintech and cryptocurrency industry, the requirement to obtain licenses in all states and territories that require it can be much more cumbersome than federal compliance — to the extent that it may have a chilling effect on innovation.[21] Through the Multistate Compact, regulators in Georgia, Illinois, Kansas, Massachusetts, Tennessee, Texas, and Washington announced their agreement that if one state reviews key elements of state licensing for a money transmitter (*e.g.,* IT, cybersecurity, business plan, background check, and compliance with the BSA), then the other participating states agree to accept the findings. The plan is that this process will significantly streamline the application and review process for both regulatory agencies and applicants. The Multistate Compact is the first step among regulators to move towards an integrated, 50-state system of licensing and supervision of fintech companies. More detail on state licensing requirements is provided below.

State financial regulators, such as the Department of Financial Services in New York and the Department of Financial Institutions in Washington State, conduct regular examinations of money transmitter businesses and may bring regulatory enforcement actions involving monetary fines, suspension or revocation of licenses, or other injunctive relief.

17 Benjamin Lo, *Fatal Fragments: The Effect of Money Transmission Regulation on Payments Innovation,* 18 Yale J. L. & Tech. 1 (2016).
18 Nat'l Multistate Licensing Sys., *Organizational Chart,* https://nationwidelicensingsystem.org/about/Pages/OrgChart.aspx (last visited Oct. 19, 2018).
19 *Model Regulatory Framework for Virtual Currencies,* CSBS (Mar. 30, 2017), https://www.csbs.org/model-regulatory-framework-virtual-currencies; State Regulatory Requirements for Virtual Currency Activities CSBS Model Regulatory Framework, CSBS (Sept. 15, 2015), https://www.csbs.org/sites/default/files/2017-11/CSBS-Model-Regulatory-Framework%28September%2015%202015%29.pdf.
20 State Regulatory Requirements For Virtual Currency Activities CSBS Model Regulatory Framework, CSBS (Sept. 15, 2015), https://www.csbs.org/sites/default/files/2017-11/CSBS-Model-Regulatory-Framework%28September%2015%202015%29.pdf.
21 Tim Fernholz, *The Patchwork of Regulations Entangling Square, and Every American Internet Startup That Takes Money,* Quartz (Mar. 14, 2013), https://qz.com/62265/why-square-and-seven-other-finance-start-ups-got-run-out-of-illinois/.

2. STATE ATTORNEYS GENERAL AND LOCAL PROSECUTORS

State Attorneys General are empowered to investigate and bring suit against individuals and financial institutions that violate the state's laws and regulations. While state Attorneys General offices vary in terms of the scope of their criminal enforcement authority, individuals or businesses that engage in money laundering activity may be subject to either criminal or civil penalties pursuant to money laundering laws or to other statutes involving fraud, tax, or consumer protection.[22] Local district attorneys' offices also have jurisdiction to bring criminal prosecutions for money laundering violations under local and state laws.

V. ACTIVITY THAT IS SUBJECT TO REGULATION

For businesses that are engaging in financial services of any kind, a key threshold question is whether these activities are of the nature that they are subject to regulation by a federal or state agency such that they require the development of a comprehensive AML Compliance program. Businesses that, for example, offer cryptocurrency exchange services, issue their own tokens, provide lending services, operate a futures trading platform, or offer or provide blockchain-based non-financial services, will all require different analyses. Some aspects of a blockchain business's business model may be regulated by multiple regulators while other parts of the business model may not be subject to any regulation. Conduct involving cryptocurrency generally falls into one of four buckets of transactions: (i) direct purchases (*i.e.*, exchanging tokens for fiat currency); (ii) direct sales (*i.e.*, exchanging tokens for tokens); (iii) custodial wallets (*i.e.*, the service of holding the private key for the individual owner, thereby holding the value contained within that key on behalf of the owner); and (iv) facilitating trades between users (*i.e.*, the trade of one token for another token). Identifying the specific regulated activity is key to determining the proper scope of the corresponding AML Compliance program that must be developed and enacted by the business. There is no one-size-fits-all AML Compliance program. All programs need to be designed to address the specific nature of the business's services offered and the risk factors associated with those services and potential customer base.

A. FEDERAL MONEY TRANSMITTING

First, if a business is engaged in "money transmitting," which is a form of regulated "money services business" ("MSB") activity under the BSA, it is considered a "financial institution" under the BSA. A person or entity is a "money transmitter" when they

1. accept "currency, funds or other value that substitutes for currency from one person" and transmit "currency, funds, or other value that substitutes for currency to another location or person by any means" or
2. are "engaged in the transfer of funds."[23]

---

22 *See e.g.*, Iowa Dept. of Justice, *Western Union to Enhance Anti-Wire Fraud Program and Pay $5 Million through 49-State Consumer Fraud Agreement,* (Jan. 31, 2017), https://www.iowaattorneygeneral.gov/newsroom/western-union-to-enhance-anti-wire-fraud-program-and-pay-5-million-through-49-state-consumer-fraud/; Western Union, *Arizona Attorney General's News Release on Multi-State Settlement,* (Feb. 11, 2010), http://ir.westernunion.com/news/archived-press-releases/press-release-details/2010/Arizona-Attorney-Generals-News-Release-on-Multi-State-Settlement/default.aspx.

23 31 C.F.R. § 1010.100(ff)(5).

MSBs must register with FinCEN and comply with various federal AML and know-your-customer requirements (commonly referred to as "KYC") as well as recordkeeping and reporting requirements. Further, operating as an unlicensed MSB may result in civil and potentially criminal penalties under federal law.

In 2013, FinCEN first issued interpretive guidance to address how its regulations apply to persons administering, exchanging, or using virtual currencies. FinCEN's guidance on virtual currencies ("Virtual Currency Guidance") interprets the money transmitter definition as encompassing products it refers to as "convertible virtual currency" and entities that are either "administrators" or "exchangers" of such virtual currency.[24]

In this guidance, FinCEN defines an "administrator" as "a person engaged as a business in issuing (putting into circulation) a virtual currency, and who has the authority to redeem (to withdraw from circulation) such virtual currency."[25] An "exchanger," on the other hand, is more broadly defined as "a person engaged as a business in the exchange of virtual currency for real currency, funds, or other virtual currency." The definition of "exchanger" is the key term for platforms that permit trades of virtual currency for other virtual currency.

Notably, the Virtual Currency Guidance further states that an administrator or exchanger that "buys or sells virtual currency for any reason is a money transmitter," unless an exemption applies.[26] Although there are reasonable bases for arguing that this language should be interpreted more narrowly, in light of underlying (and controlling) FinCEN regulations and subsequent FinCEN administrative rulings, it does tend to indicate FinCEN's general intention to broadly regulate virtual currency activity within its regulatory jurisdiction.

VIRTUAL CURRENCY (in contrast to "real currency")

A medium of exchange that operates like a currency in some environments, but does not have all the attributes of real currency; specifically, virtual currency lacks the status of legal tender in any jurisdiction.

FinCEN defines "virtual currency," in contrast to "real currency," as "a medium of exchange that operates like a currency in some environments, but does not have all the attributes of real currency;" specifically, virtual currency lacks the status of legal tender in any jurisdiction. Since this time, FinCEN has issued additional guidance clarifying its stance on activities in this industry.

24 *See* Dep't of Treas., Financial Crimes Enforcement Network, *Application of FinCEN's Regulations to Persons Administering, Exchanging, or Using Virtual Currencies,* FIN-2013-G001 (March 18, 2013), https://www.fincen.gov/sites/default/files/shared/FIN-2013-G001.pdf. (hereinafter "Virtual Currency Guidance").
25 *Id.* at 2.
26 *Id.* at 3.

The Virtual Currency Guidance is limited to "convertible" virtual currency, which means a virtual currency that has "an equivalent value in real currency, or acts as a substitute for real currency." The threshold question then, for an analysis of Exchanger or Administrator compliance responsibilities with respect to any given token issuer, will almost always be whether the token sold constitutes a "convertible" virtual currency. If not, the issuer or exchanger would not likely be considered an MSB because it is not issuing or exchanging convertible virtual currency.

On May 9, 2019, FinCEN issued guidance regarding the "Application of FinCEN's Regulations to Certain Business Models Involving Convertible Virtual Currencies" (the "2019 Guidance").[27] While the 2019 Guidance purports to "not establish any new regulatory expectations or requirements," it delves into a number of specific applications and uses of convertible virtual currencies, and the application of certain requirements under the BSA.

Specifically, it reaffirms the principle of a strong "culture of compliance" and the need for a risk assessment to tailor AML compliance programs to mitigate known risks. In addition, for the first time, FinCEN details its views on the applicability of the Funds Transfer Rule and Funds Travel Rule to convertible virtual currency transactions, finding that they do apply to transfers of convertible virtual currency between financial institutions.

The 2019 Guidance also describes the application of specific business models involving the transmission of convertible virtual currency:

P2P Exchanges — BSA typically will apply unless involves a natural person engaging on an infrequent basis and not for profit or gain.

Wallets —

- "Hosted" wallets — typically hold customer funds and thus are money transmitters.
- "Unhosted" wallets — typically considered a "user" and thus not a money transmitter.
- Multi-signature wallet providers — if provided in conjunction with a hosted wallet, may be a money transmitter; if provided for an unhosted wallet, likely not a money transmitter.

ATMs/Kiosks — an owner/operator who uses the terminal to receive Convertible Virtual Currency and transmit it is a money transmitter for both transactions (receiving and transmitting).

27 *Application of FinCEN's Regulations to Certain Business Models Involving Convertible Virtual Currencies*, FIN-2019-G001, Fin. Crimes Enf't Network (May 9, 2019), https://www.fincen.gov/resources/statutes-regulations/guidance/application-fincens-regulations-certain-business-models .

Decentralized Applications (DApps) — the 2019 Guidance simply says that, similar to kiosks, when DApps perform money transmission services, the BSA will apply to the DApps, the owners/operators of the DApp, or both.

Anonymity-Enhanced Transactions —

- Anonymizing services provider — if they accept and transmit value, they are a money transmitter; the provision of privacy mechansims does not change the analysis nor does it qualify for the "intergral" exception.
- Anonymizing software provider – not a money transmitter pursuant to the exemption for delivery, communication, or network services access used by a money transmitter to support money transmission services. Note the user of the software may be a money transmitter.
- Providers of anonymity-enhanced Convertible Virtual Currencies (privacy coins) — may be a money transmitter if it acts as an administrator of a centralized Convertible Virtual Currency system and issues Convertible Virtual Currency in exchange for payment; uses such Convertible Virtual Currency to pay for goods and services typically not money transmitters; develops of decentralized Convertible Virtual Currency payment systems if accepts and transmits value.
- Money transmitters that accept or transmit anonymity-enhanced Convertible Virtual Currencies — FinCEN notes that these organizations must comply with the Funds Travel Rule and determine the identity of transmittors or recipients.

Payment Processors — are money transmitters and not eligible for the payment processor exception.

Internet Casinos — if not considered a "casino" under the BSA, may still be considered a money transmitter.

Models That May Be Exempt —

- Trading Platforms and Decentralized Exchanges — may be exempt if the parties to the transaction settle the trade themselves (off the platform).
- Initial Coin Offerings.
  - At Issuance — generally the issuer acts as an administrator at the time of issuance. Nevertheless, exceptions may apply, including when: a) they are a bank or registered with, and functionally regulated or examined by, the SEC or CFTC, and b) the fundraising activity falls under the integral to the sale of goods and services exemption, unless the asset serves as value that substitutes for currency.
  - Purchase or Resale — Generally, resale by the investor does not create BSA obligations for the investor. (Note if SEC or CFTC jurisdiction applies, other requirements will be triggered.)
  - DApp Developer — Dapps financed through ICO fundraising activity consists of the production of goods and services and is not money transmission. If deployed to engage in money transmission, then will qualify as a money transmitter.
  - DApp User — if deployed to engage in money transmission, then will qualify as a money transmitter.
  - Pre-mining — if used to pay for goods and services, or repay obligations (such as amounts owed to project investors), then not money transmission.
- Mining Pools — typically not money transmitters but will be if host a wallet on behalf of pool members or contract purchasers.

The list represents a summary of the 2019 Guidance. If you have a particular use case that falls within one of the above categories, please consult the Guidance directly.

If you are selling a token, issuing a token, or exchanging tokens for cryptocurrency or fiat currency, it is advisable to consult counsel to evaluate your particular services and payment flows, and help determine if your organization should register with FinCEN.

B. STATE MONEY TRANSMITTING

1. WHAT STATES GENERALLY REGULATE

States regulate a broad range of conduct under money transmitter laws. The traditional conduct known as “money transmission” accepts currency, funds, or value from one person in order to transmit that value to another location or person by any means. State laws on money transmission vary widely but can generally be grouped into several categories. Most states define money

transmission as including some or all of three types of activities: (1) the receipt of money or monetary value for transmission, (2) issuing and/or selling payment instruments, and (3) issuing and/or selling stored value. Currently, 49 states plus the District of Columbia regulate money transmission. Many of these states only regulate these activities when "money" is involved, which is generally defined as "a medium of exchange that is authorized or adopted by a domestic or foreign government."[28] State statutes with this limitation will not, by their own terms, govern activities involving virtual currencies exclusively, which are not adopted by any domestic or foreign government.[29]

Some states have taken a position that the state will not regulate transactions involving cryptocurrencies or digital assets. Other states' money transmitter laws define "currency" to only include government-backed monetary value (or fiat currency). Some state money transmitter statutory schemes have broader definitions of "currency" that would include value represented by cryptocurrency or digital assets. Finally, some states have adopted legislation or have taken positions directly addressing how cryptocurrency, virtual currency, digital currency, or digital assets will be treated in that state.[30]

Some states have promulgated exceptions to their money transmitter licensing laws and regulations that, if applicable to a particular company, can ease the burdens of complying with the patchwork of existing state money transmitter laws. However, the substantial variation in how states have interpreted and applied their exceptions means that a careful state survey is prudent before a company determines that it will not register as a money transmitter if it conducts these activities in a particular state.

If you are selling, storing, or trading a token, especially if the token functions as a means of moving monetary value, you will likely need to be licensed to operate in the various states, and you should analyze your business model and payment flows on a state-by-state basis. Please consult an attorney to review the flow of funds for your particular operation in order to determine where you need to apply for licensure.

2. STATE LICENSING (CONSUMER PROTECTION) VS. FEDERAL REGISTRATION

Money transmission is regulated at both the federal and state levels, but for different reasons, and with a different focus. Federal registration with FinCEN is focused on combatting money laundering efforts throughout the world. To register with FinCEN, your organization must have an

28 Note that Oregon is an exception — defining "money" as "a medium of exchange that: (a) The United States or a foreign government authorizes or adopts; or (b) Represents value that substitutes for currency but that does not benefit from government regulation requiring acceptance of the medium of exchange as legal tender." Or. Rev. Stat. § 717.200.

29 *See, e.g.,* Texas Dept. of Banking, *Supervisory Memo. - 1037* (updated Jan. 2, 2019), https://www.dob.texas.gov/public/uploads/files/consumer-information/sm1037.pdf (noting that "[b]ecause neither centralized virtual currencies nor cyptocurrencies are coin and paper money issued by the government of a country, they cannot be considered currencies under the statute. Therefore, absent a legislative change to the statute, no currency exchange license is required in Texas to conduct any type of transaction exchanging virtual with sovereign currencies."). Texas' guidance provides a similar analysis regarding money transmission ("Because cryptocurrency is not money under the Money Services Act, receiving it in exchange for a promise to make it available at a later time or different location is not money transmission."). Under this guidance, the analysis may change when a cryptocurrency transaction involves sovereign (fiat) currency.

30 States that have directly addressed how the state will handle cryptocurrencies (either by statutory amendment or formal guidance) include: Alabama, Colorado, Connecticut, Georgia, Illinois, Kansas, New Hampshire, New Mexico, New York, North Carolina, Pennsylvania, South Carolina, Tennessee, Texas, Washington, and Vermont.

AML compliance program and processes in place to catch suspicious activities that may be related to money laundering.

In contrast to federal requirements, the 50-state money transmitter licensing regime is aimed more at consumer protection by making sure that companies who receive funds from consumers protect, store, and transmit those funds safely, securely, and accurately. That said, all states also view their licensing oversight as complimentary to and supportive of federal AML goals; and some states even have integrated AML compliance obligations into their money transmission licensure requirements.

The application process to obtain a money transmitter license in each state is far more onerous than registering with FinCEN. States look into the company's finances (including historical finance report), litigation history, criminal history, bankruptcy history, employment history of controlling persons, among a plethora of other information.

C. SECURITIES OR COMMODITIES

Although SEC officials have stated that some cryptocurrencies such as bitcoin and ether are not securities subject to SEC oversight, it does assert jurisdiction over most, if not all, ICOs which it believes are methods to raise capital by issuing securities that must be registered unless an exemption to the registration requirement applies.[31] A determination of whether a token or coin is a security depends on an application of the *Howey* Test.[32] Pointing to *Howey*, the SEC has stated that, to the extent a token or coin is offered or sold in a way that causes investors to have a reasonable expectation of profits based on the efforts of others, it is a security; and it sees most token or coin sales as fitting that description.[33] Consistent with this position, the SEC has brought enforcement actions aimed at enforcing registration requirements for securities related to ICOs.[34] Similarly, while the CFTC generally recognizes the SEC's jurisdiction over ICOs, it asserts its own jurisdiction over virtual currency derivatives and in instances where there is fraud of manipulation involving virtual currency markets.

It is worth noting that FinCEN regulations specifically provide that businesses "registered with, and functionally regulated or examined by" either the SEC or CFTC are excluded from the class of "money services businesses" that are regulated by FinCEN. (Such organizations will be subject to the AML requirements of the SEC or CFTC.) However, in practice, there currently exists a substantial lack of clarity about what the lanes of each of the federal regulators are and whether there will continue to be overlapping assertions of jurisdiction.

1. AML REQUIREMENTS APPLICABLE TO REGULATED BLOCKCHAIN COMPANIES

A business that is conducting activity that is regulated by any federal regulator must develop and maintain an AML program that meets the same general criteria. Most broadly, businesses that

31 Spotlight on Initial Coin Offerings (ICOs) , Sec. and Exchange Comm'n, https://www.sec.gov/ICO (last visited Aug. 15, 2019).
32 *SEC v. W.J. Howey Co.*, 328 U.S. 293 (1946).
33 William Hinman, Digital Asset Transactions: When Howey Met Gary (Plastic), Remarks at the Yahoo! Finance All Markets Summit: Crypto (June 14, 2018), The DAO, Exchange Act Release No. 81207 (July 25, 2017), https://www.sec.gov./litigation/investreport/34-81207.pdf .
34 SEC Annual Report, Division of Enforcement, 7. https://www.sec.gov/files/enforcement-annual-report-2018.pdf.

are subject to the regulatory requirements discussed above are required to develop, implement, and maintain an effective anti-money laundering program reasonably designed to prevent the money services business from being used to facilitate money laundering and the financing of terrorist activities.[35]

Those businesses that engage in money transmitting or other money services under federal law are required to register with FinCEN, which involves the submission of an electronic form on FinCEN's website[36] to provide information about the business, including: identification of the business's owner or controlling person, type of money services being provided, location of business, and bank account information for the business's primary transaction account.

To meet AML requirements, a business must have a formal AML compliance program that includes the following four elements: 1) written policies and procedures; 2) a designated AML compliance officer; 3) independent review and monitoring of the AML program, and 4) a training program for relevant personnel regarding their AML responsibilities. Additionally, money services businesses are subject to a number of reporting and record-keeping requirements, particularly, the requirement to file Suspicious Activity Reports, or "SARs", for transactions over $2,000 that appear to involve funds from illicit activity, be designed to evade reporting requirements under the BSA, or serve no apparent lawful or business purpose.

Although it may be possible to assign the responsibilities for your AML compliance program to a founder, manager, or employee with other duties if your business does not currently support a stand-alone function, keep in mind that it is critical that this function be resourced and, most importantly, free from the influence of the business or sales side of the organization.

Many participants in the cryptocurrency and token sale marketplace are based outside of the United States. If a company has what FinCEN refers to as foreign "agents," a term it uses to include "authorized delegates, foreign agents or counterparties, agents, and sub-agents," the business' AML program must meet additional requirements. For example, if there is a contractual arrangement to make tokens available to a foreign company or its customers through the foreign company's software platform, you must:

- conduct due diligence on foreign agents and counterparties;
- consider a number of particular risk factors and conduct risk-based monitoring of your agents and counterparties, and;
- develop and implement a policy for corrective action and termination for non-compliant entities.

35 31 C.F.R. § 1022.210.
36 Money Services Business (MSB) Registration, Fin. Crimes Enf't Network, https://www.fincen.gov/money-services-business-msb-registration (last visited Aug. 15, 2019).

VI. GUIDELINES BASED ON LESSONS FROM ENFORCEMENT, EXPERIENCE WITH REGULATORS, AND BEST PRACTICES

Blockchain and virtual currency companies are no longer completely novel. State and federal regulators have started issuing guidance, bringing enforcement actions, and amending their statutes and regulations to address it. The following section provides some high-level guidelines for token issuers and operators of businesses that trigger AML laws and regulations and need to demonstrate appropriately calibrated compliance.

A. CREATE A STRONG CULTURE OF COMPLIANCE WITH A SUPPORTIVE TONE FROM THE TOP

FinCEN's guidance emphasizes the importance of a culture of compliance.[37] The agency's view is that "[r]egardless of its size and business model, a financial institution with a poor culture of compliance is likely to have shortcomings in its BSA/AML program."[38] To this end, the agency recommends active engagement at a company's leadership and board levels, and makes clear that "[t]he commitment of an organization's leaders should be visible within the organization, as such commitment influences the attitudes of others within the organization."[39] Consistent with these principles, the agency has initiated enforcement actions against financial institutions that fail to promote effective information sharing between the company's AML Officer and its leadership.[40]

B. DEVELOP A COMPREHENSIVE COMPLIANCE PROGRAM

Any entity that registers as an MSB with FinCEN, applies for state money transmitter licenses, or identifies a need to implement AML compliance procedures should identify and designate a BSA/Compliance Officer early in the business's development stage. This role can be filled initially by someone with other duties but will ultimately need to be undertaken by someone with experience and knowledge of AML rules and regulations. An effective compliance program is based on a comprehensive assessment of relevant risks and tailored to mitigate or eliminate those risks. Third-party service providers who help perform AML or other compliance functions (like OFAC screening services and identity verification providers) should be clearly and intentionally integrated into the compliance program and service providers should perform their services free from undue influence from the business, marketing, or sales sides of the organization (who may encourage cutting corners on KYC to improve onboarding and customer retention metrics). These third parties should be carefully vetted to ensure that they reliably perform their advertised services. You should audit that compliance early and often.

37 FinCEN, *Advisory to U.S. Financial Institutions on Promoting a Culture of Compliance*, FIN-2014-A007 (Aug. 11, 2014).
38 *Id.*
39 *Id.*
40 *See, e.g., In the Matter of First Bank of Delaware,* No. 2012-01 (Nov. 19, 2012) (explaining that "the Bank's Board and other appropriate Bank personnel were not notified of numerous instances of potential suspicious activity" related to the MSB business line, and that "the BSA Officer failed to escalate BSA problems to senior management").

C. EMPOWER THE AML/COMPLIANCE OFFICER WITH RESOURCES AND AUTHORITY TO REMEDY PROBLEMS

FinCEN has also made clear the importance of granting the AML Officer sufficient resources and authority to effectively monitor the AML risks present in a company's business model, as well as adequate authority to ensure any deficiencies are promptly redressed.[41] This is critical because "[t]he failure of an institution's leaders to devote sufficient staff to the BSA/AML compliance function may lead to other failures" — such as the inability to monitor transactions and accounts or to ensure timely filing of SARs.[42] Again, FinCEN has supported this guidance with enforcement actions that target companies with insufficiently resourced and staffed AML programs.[43]

D. ENABLE FLOW OF REPORTING BETWEEN BUSINESS UNITS AND AML OFFICER

FinCEN's guidance specifically criticizes companies that fail to adequately share information between their AML departments and other relevant units within the business.[44] In 2014, FinCEN noted a troubling trend in information silos within organizations that ultimately precluded AML departments from obtaining sufficient information to effectively carry out their BSA responsibilities. Again, in this space, FinCEN's warnings have been preceded and followed by enforcement actions targeting companies that have inadequately developed reporting processes by which relevant information can flow between the AML Officer and the business.[45]

E. CONDUCT EFFECTIVE CUSTOMER ONBOARDING/KYC

The regulations governing MSBs require them to implement written AML compliance programs that incorporate policies and procedures reasonably designed to effectively "verify" customers' identification.[46] The extent and thoroughness of the verification requirement is not specified in the MSB regulations. That said, an entity's procedures must be appropriately tailored to the money laundering risk associated with the platform, the customer, and the transaction.

It is generally viewed as insufficient to collect only the name and email address of a customer. Further, entities should request the name and physical address of a customer and confirm such information by viewing an appropriate and valid identification document. Entities should establish systems (whether manual, automated, or both) to verify that all required identification data fields are completed and

41 FinCEN, *Advisory to U.S. Financial Institutions on Promoting a Culture of Compliance*, FIN-2014-A007 (Aug. 11, 2014).
42 *Id.*
43 *In the Matter of: U.S. National Bank Association*, No. 2018-01 (FinCEN Feb. 15, 2018) ("Appointing a BSA officer is not sufficient to meet the regulatory requirement if that person does not have sufficient authority, resources, or time to satisfactorily complete the job."); Deferred Prosecution Agreement Statement of Facts, *U.S. v. HSBC Bank USA, N.A.*, 1:12-cr-00763-ILG (E.D.N.Y. Dec. 11, 2012) (ECF No. 3-3) (faulting HSBC for combining the roles of General Counsel and AML Compliance Officer).
44 Fin. Crimes. Enf't Network, *Advisory to U.S. Financial Institutions on Promoting a Culture of Compliance,* FIN-2014-A007 (Aug. 11, 2014) ("Several recent enforcement actions noted that the subject institution had relevant information in its possession that was not made available to BSA/AML compliance staff. This may have resulted from a lack of an appropriate mechanism for sharing information, a lack of appreciation of the significance or relevance of the information to BSA/AML compliance or an intentional decision to prevent compliance officers or staff from having access to the information.")
45 *In the Matter of Oppenheimer,* No. 2015-01 (Jan. 26, 2015) ("[Di]vision of responsibility [between the AML Group and Surveillance Group] and the resultant silos of information contributed to the Firm's failure to identify and investigate the suspicious . . . activity at issue in this matter."); *In the Matter of Thomas Haider*, No. 2014-08 (Dec. 18, 2014) ("This arrangement — maintaining separate 'silos' of information within [MSB's] various departments such that [its] SAR analysts did not possess relevant information — was in place throughout [the CCO]'s employment."); *In the Matter of American Express Bank Int'l,* No. 2007-01 (Aug. 3, 2007) (explaining compliance responsibilities were insufficiently defined and implemented with respect to "escalating or sharing identified negative customer information among appropriate personnel at the Bank.").
46 *See* 31 C.F.R. § 1022.210(d)(1)(i)(A).

that false names (such as Donald Duck or Satoshi Nakamoto) are captured and reviewed. In such instances, the entity should have procedures in place that designate the required information and documentation to be provided and steps to take to determine whether to deny the application or shut the account, as appropriate.

When dealing with non-natural persons, such as legal entities, MSBs should develop appropriate customer onboarding procedures to vet and verify corporate records necessary to validate prospective corporate or enterprise customers. For example, MSBs should require identification documentation to confirm the identities of the ultimate beneficial owners of the company. They should also request corporate articles of incorporation, bylaws, and lists of Board members. Care should be taken to understand the ultimate source of funds for corporate or enterprise customers and to ensure that the company is not unwittingly allowing illicit funds to pass through its platform under the guise of corporate or wholesale transactions.

Finally, entities should devise and frequently test their verification procedures to ensure they are reliable and effective and make corrections or updates where needed.

F. CONDUCT VIGILANT TRANSACTION MONITORING AND SAR FILING

FinCEN has initiated a significant number of enforcement actions upon determination that a company failed to adequately monitor transactions for suspicious activity,[47] and in turn failed to timely file SARs as required by the BSA and its implementing regulations.[48]

Not only are the above offenses subject to criminal or civil prosecution, but the proceeds of criminal activity, and any property "involved" in a money laundering offense that may include such things as non-tainted funds in the same account, commissions or fees, websites, or even an entire business, are subject to criminal or civil forfeiture.

State regulators, New York in particular, are increasingly insistent that licensees involved in the blockchain space develop and maintain processes and procedures to effectively monitor transactions to identify, prevent, and report suspicious activity. These obligations, while not required by any specific statutory requirement, can be imposed in supervisory agreements or additional guidance.

Transaction monitoring should be a mixture of automated and manual processes, tailored to individual circumstances, but aimed at effective identification and prevention of use of the services to launder money or commit or facilitate crime. As with the use of third-party service providers for other aspects

47 *In re King Mail & Wireless, Inc.*, No. 2015-06 (June 1, 2015) (finding the MSB liable for failing to report "multiple wire transfers that were conducted on the same day, or within a few days of each other, and in amounts that [individually] would not trigger the recordkeeping requirements"); *In re Gibraltar Private Bank & Tr.*, No. 2016-01 (Feb. 25, 2016) (finding bank liable for a "transaction monitoring system contain[ing] account opening information and customer risk profiles that were frequently incomplete, inaccurate, and lacked sufficient analysis and validation").

48 *In re U.S. Bank,* No. 2018-01, (Feb. 15, 2018) (finding bank liable for "capping the number of alerts its automated transaction monitoring system would generate for investigation . . . caus[ing] the Bank to fail to investigate and report large numbers of suspicious transactions"); *In the Matter of W. Union Fin. Servs.*, No. 2017-01 (Jan. 19, 2017) (finding an MSB liable for taking "over 90 days to investigate activity for which it had facts to constitute the basis for filing a SAR"); *First Nat'l Cmty. Bank,* No. 2015-03, at 3-4 (Feb. 27, 2015) (failure to file SARs for activity related to a subpoena about a certain customer "deprived law enforcement of information that may have assisted law enforcement in tracking millions of dollars in related corrupt funds"); *In re Haider*, No. 2014-08 (Dec. 18, 2014) (finding that "individuals responsible for filing SARs were not provided with information possessed by [the company's] Fraud Department that should have resulted in the filing of SARs").

of compliance, entities should take great care not to rely solely on third parties for transaction monitoring, as that responsibility lies primarily with the MSB or licensed money transmitter and cannot be fully outsourced.

G. CONDUCT APPROPRIATE SANCTIONS SCREENING

Even if the BSA is not triggered by your activities, OFAC sanctions prohibitions still apply. This means that you must know your counterparties to avoid inadvertently providing or facilitating the financing of terrorism or other sanctioned persons or entities. Screening activity should be tailored to the risk presented by your platform.

TOKEN ALLIANCE

CHAMBER OF DIGITAL COMMERCE

UNDERSTANDING DIGITAL TOKENS

Considerations and Guidelines for Advancing Cybersecurity in the Token Economy

Prepared by the Token Alliance – an industry initiative of the Chamber of Digital Commerce

SECOND EDITION • SEPTEMBER 2019

CONSIDERATIONS AND GUIDELINES FOR ADVANCING CYBERSECURITY IN THE TOKEN ECONOMY

The Chamber of Digital Commerce would like to thank the following individuals and organizations for their valuable contributions to the Token Alliance in the production of this report.

We would also like to extend a special thank you to **Sal Ternullo and Sam Wyner, Directors and Cryptoasset Services Co-Leads of KPMG LLP,** for helping to lead the development of this report.

PAUL BRIGNER
Chamber of Digital Commerce

STEVE BUNNELL
O'Melveny & Myers

DAVID FITZGERALD
O'Melveny & Myers

AMY DAVINE KIM
Chamber of Digital Commerce

OLGA MACK
Quantstamp

RAMESH NAGAPPAN
Harvard University

DIVIJ PANDYA
Chamber of Digital Commerce

STEVEN SPRAGUE
Rivetz

COLLEEN SULLIVAN
CMT Digital

DAWN TALBOTT
RiskSpan

TABLE OF CONTENTS

II. INTRODUCTION

This new installment of our series of reports is an important addition to the overall regulatory and market consideration of the token ecosystem. The way in which digital tokens operate is complex and can maintain multiple characteristics – from an investment contract, to something necessary for utilizing a digital platform, to a form of payment or exchange, to name just a few. We are in a moment when technological advancement is pushing the boundaries of decades-long established law – law that was made at a time when tokenized assets and instantaneous digital transfers of value were not contemplated. It is exciting to be a part of it, but it also entails risks.

To facilitate the development of token businesses as well as minimize incidents of fraud and compliance challenges, the Chamber embarked on a plan to tackle each of the issues impacting this ecosystem. This journey started with a publication of guidelines for digital tokens that were intended to operate outside Securities and Exchange Commission (SEC) and Commodities Futures Trading Commission (CFTC)-regulated products and services laws (so-called "utility tokens" and associated platforms).

Those Guidelines also sought to provide legal context by detailing the legal landscapes governing digital tokens in five countries – the United States, Canada, the United Kingdom, Australia, and Gibraltar. Taking up a sizeable portion of the Report, the description of the vast number of potential legal requirements and government oversight demonstrated that this is a regulated industry, no matter where you fall in the spectrum of token categorization.

Finally, we provided an economic perspective on the industry with an analysis of market trends. The sheer volume of capital raised demonstrates the passionate interest of so many around the world in the potential of these markets – whether as a way to make money, a way to use new and better services, or other reasons. This installment expands on those initial resources to balance out the conversation around utility tokens to discuss the rules, regulations, and resulting considerations for those who wish to issue or trade tokens that are or otherwise represent securities. This sector of the market is growing with entrants from new technology companies as well as established institutional financial services providers. The securities laws are complex, generated in the 1930s and developing substantial legal and regulatory precedent. In some cases, that precedent has endured because it is principles-based. In others, it has become outdated as it no longer sufficiently contemplates the types of securities that can be created, issued, held, and traded digitally.

We are excited to introduce these guidelines for cybersecurity related to digital tokens. First, these guidelines address cybersecurity considerations for public blockchains. These considerations account for the issues associated with a lack of central authorities, attack vectors in a consensus driven system, and other challenges unique to the blockchain environment. Second, the guidelines explore regulatory considerations from a cybersecurity perspective, addressing the application of both new and existing frameworks. Third, and finally, we provide a set of guidelines for advancing cybersecurity in a tokenized economy.

While this document primarily focuses on cybersecurity risks and associated guidelines to address them, blockchain technology is a major step forward from a cybersecurity perspective. Blockchain is based on the discovery of new ways to leverage existing cybersecurity technologies like public key cryptography, distributed computing, and consensus mechanisms to create ledgers that feature inherent tamper resistance and resiliency never before realized with traditional approaches. Because of its cybersecurity and other benefits, many experts foresee a time when blockchain will underpin all of our enterprise business models, and we anticipate publishing additional papers to further explore the cybersecurity benefits of blockchain technology.

This report complements our recent work on consumer protection and securities and non-securities tokens. But we can't stop there. More areas need to be considered and addressed with thoughtful analysis. We will be supplementing our legal landscape on a rolling basis with the introduction of additional countries and the laws that apply to digital tokens.

We hope you enjoy these publications and that they serve to help guide your analysis and views of the evolving digital token ecosystem. We look forward to sharing this series as we roll out these publications throughout the coming weeks!

A few words of caution:

THIS REPORT DOES NOT CONSTITUTE LEGAL ADVICE

- Specifically, nothing in this report should be construed as advice regarding the law of the United States or any other jurisdiction.
- This report, including its suggested guidelines, merely express the general views of the Token Alliance, and compliance with such guidelines cannot assure that the distribution or trading of tokens will fully comply with the laws discussed herein.
- These views are being offered for discussion purposes only, and they have not been sanctioned by any regulator or government agency.

CONSULT LEGAL COUNSEL BEFORE DISTRIBUTING OR HOSTING TRADES OF DIGITAL TOKENS

- Token Sponsors and associated parties seeking to generate or distribute a blockchain-based token should seek independent legal counsel with expertise in this area before proceeding with their project, particularly given the fast-paced nature of this industry and the quickly evolving legal landscape.
- Counsel can help consider the facts and circumstances surrounding particular issues within the contours of then-current regulatory and enforcement activity.
- This report does not attempt to address any individual case, and the thought leadership contained herein is not appropriate for use as a substitute for independent counsel.
- Further, the digital token market is rapidly shifting and therefore the cases and regulatory interpretations discussed in this report may be overtaken by future events.

The Token Alliance will continue to study the issues surrounding the appropriate regulation for tokens and it will offer additional insights, as appropriate, when new developments arise.

III. GUIDELINES FOR ADVANCING CYBERSECURITY IN A TOKENIZED ECONOMY

A. INTRODUCTION

The digital economy continues expanding across technology domains and industry lines, driving economic growth and enhancing consumer experiences. In this era of digital innovation, blockchain is one of the most progressive examples of technology convergence at the intersection of applied cryptography and distributed systems. Blockchain has inspired the emergence of fundamentally new assets, and, in parallel, has encouraged innovators to reimagine how traditional assets are issued, managed, exchanged, and accounted for. Although still in early days, investment into blockchain innovation and development has increased dramatically with innovators striving to realize blockchain's potential to become a foundational technology layer of a digitized economy.

While the market continues to place a strong focus on blockchain's transformative potential, there has been less focus on blockchain cyber risks and benefits. This phenomenon is ironic given blockchain technology is best known for giving rise to "cryptocurrencies," where "crypto" describes the application of cryptographic functions and mechanisms to support secure transactions recorded on a decentralized ledger. The use of cryptographic functions and distributed architectures enable key blockchain value drivers including tamper resistance and resiliency. The inherent composition and structure of the technology that links blocks of transactions cryptographically — creating the "chain" in "blockchain" — makes them tamper–resistant. In other words, attempts to modify a blockchain ledger (whether maliciously or otherwise) are extremely difficult and, if somehow successful, open and conspicuous. Also, the fact that blocks are cryptographically linked sequentially eliminates the availability of large troves of data such that a malicious actor would need not only modify the transaction they seek to alter, but every transaction thereafter in order to hide the change. The power and rate of computing ability needed to accomplish such a task has thus far proved impossible for the Bitcoin blockchain. These attributes can be widely applied to solve data problems persistent in current computing models across industries in managing data integrity, availability, and transparency.

In 2018, Microsoft partnered with the Chamber of Digital Commerce to publish "Advancing Blockchain Cybersecurity," which discussed permissioned blockchain "capabilities in mitigating cybersecurity risks and detecting, preventing, and combatting the types of cyber-attacks that are often directed at financial institutions."[1] The paper discussed distributed architectures, consensus validation mechanisms, encryption (cryptographic immutability), transparency, and administrator risk controls. While these features were discussed in the context of permissioned blockchains, there are unique and nuanced risk considerations when considering permissionless or "public" blockchains and blockchain-enabled assets such as cryptocurrencies.

These unique risk considerations have resulted in a high frequency of cyber events with significant impacts across the tokenized economy. The ecosystem has incurred billions of dollars of cyber-related losses[2] and major insolvency events (*e.g.*, Mt. Gox and Quadriga) which have subsequently led to skepticism in both digital assets and the broader ecosystem. In this report, we will discuss these unique and nuanced risk considerations to help practitioners, policymakers, and investors across the ecosystem better understand and effectively manage cybersecurity to protect tokenized assets.

B. CYBERSECURITY CONSIDERATIONS FOR PUBLIC BLOCKCHAINS

The 2018 paper "Advancing Blockchain Cybersecurity" assessed the cyber risk profile of permissioned blockchains within the financial services industry, laying the foundation for this piece to discuss unique and nuanced risk considerations for public blockchains and enabled digital assets. The risks described in the 2018 paper focus on private key management, software and protocol vulnerabilities, external data sources and endpoint risks, data security and privacy, and evolving attack vectors, which are each applicable and relevant to public blockchains.

This report applies these risks factors and highlights unique and nuanced risk considerations for public blockchains, including:

1. Lack of central authorities and impacts to asset recoverability
2. Compromise of distributed consensus protocols
3. Inappropriate access to private keys and/or endpoints
4. Protocol and smart contract vulnerabilities
5. Inaccurate external data sources

1 Erin English, Amy Davine Kim, and Michael Nonaka, Advancing Blockchain Cybersecurity: Technical and Policy Considerations for the Financial Services Industry (2018), https://www.microsoft.com/en-us/cybersecurity/content-hub/advancing-blockchain-cybersecurity.

2 *See, e.g.*, Kate Rooney, $1.1 Billion In Cryptocurrency Has Been Stolen This Year, And It Was Apparently Easy To Do, CNBC (June 7, 2018), https://www.cnbc.com/2018/06/07/1-point-1b-in-cryptocurrency-was-stolen-this-year-and-it-was-easy-to-do.html.

1. LACK OF CENTRAL AUTHORITIES AND IMPACTS TO ASSET RECOVERABILITY

In both traditional technology environments and permissioned blockchains, central authorities control critical technology operations including identity and access management ("IAM") to control user's access to read and process information using business applications. The most important scientific breakthrough that Bitcoin provided was the ability for participants in a distributed system to perform trusted transactions and achieve consensus on the state of a distributed ledger without central authorities to facilitate settlement and mitigate counterparty risk. Bitcoin's consensus mechanism, proof-of-work ("PoW"), provided the first viable solution to achieve consensus on the state of a distributed ledger and transaction history across a network of distributed unknown participants. By doing so, Bitcoin enabled the emergence of blockchain technology unlocking the ability for counterparties to perform trusted transactions directly without central authorities, having wide-reaching implications to many businesses and industries. Within the context of this discussion, then, we focus on the risk implications that a lack of central authorities has to digital assets on public blockchains.

The comparatively rapid settlement of transactions executed on public blockchains enable counterparties to achieve nearly instantaneous settlement finality. Once a transaction is executed, whether authorized by the owner or not, and the transaction is validated by the network through consensus, the asset transfer is final, and the transaction cannot be reversed or recovered. In this regard, the "finality" condition for transactions executed on public blockchains is unique from traditional asset exchanges which are cleared through traditional financial market infrastructure, often including broker-dealers, exchanges, clearing houses and custodian banks. In traditional market infrastructure, asset owners can often pursue remediation through established asset recovery procedures or legal proceedings targeting the central authorities who facilitated the transaction. This type of action is not possible for transactions executed for assets on public blockchains because there are no central authorities. Policymakers and practitioners must consider these risk implications when designing standards and best practices for business models engaging with public blockchains and enabled assets.

There have been historical scenarios where a public blockchain community implemented a solution to achieve asset recovery when a significant negative event occurred. In 2015, following a major asset compromise via a smart contract vulnerability on the Ethereum blockchain, the community deployed a "hard fork" (protocol changes) to facilitate asset recovery. While the asset recovery was effective, the decision to deploy the hard fork was highly contentious and divisive.[3] Moving forward, it is reasonable

3 The Ethereum: Digital Autonomous Organization ("DAO") fund recovery resulted in Ethereum Classic. Antonio Madeira, *The Dao, The Hack, The Soft Fork And The Hard Fork*, Cryptocompare (Mar. 12, 2019), https://www.cryptocompare.com/coins/guides/the-dao-the-hack-the-soft-fork-and-the-hard-fork/.

to assume that hard forks will not be a viable asset recovery method until ongoing efforts in the ecosystem, such as protocol upgrades (*e.g.*, Ethereum Improvement Proposal ("EIP") #867[4]) are implemented.

In the absence of technical solutions to facilitate asset recovery following a cyber event, asset issuers and owners have pursued global coordination between exchanges to track and trace assets using analytical approaches to flag and recover assets. These approaches focus on eliminating off-ramps for malicious actors to convert compromised assets into fiat currencies.

Although this has led to successful asset recovery in several circumstances, substantial challenges are associated with this type of coordination that impede its effectiveness. It is also important to note that advanced cryptographic implementations (*i.e.*, zero-knowledge proofs or "ZKP"), as well as increasing interoperability across networks (*i.e.*, atomic swaps), may prove substantial challenges for organizations attempting to track and trace compromised assets using analytical approaches over the transaction ledger.

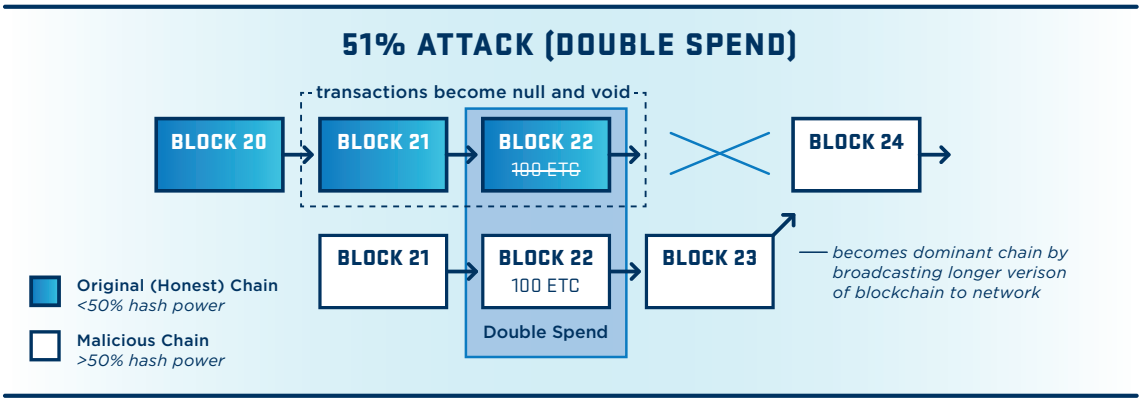
2. COMPROMISE OF DISTRIBUTED CONSENSUS PROTOCOLS

In Section A, we established consensus mechanisms as a major breakthrough and discussed the risk implications that peer-to-peer transactions have to asset recoverability in the event of a compromise due to a cyber event. In this section, we build on the discussion of consensus mechanisms to explore risks directly related to distributed consensus protocols.

Consensus mechanisms in distributed systems have been an area of scientific and academic exploration for decades, however, Bitcoin provided the first production quality solution in Proof-of-Work ("PoW"). While PoW has achieved mass adoption to date, consensus mechanisms are evolving as researchers, scientists, and the private sector focus on investment into consensus innovation. To this point, a number of public blockchain communities, including Ethereum, have communicated intentions to adopt Proof-of-Stake ("PoS") consensus models where validators "stake" their tokens as security deposits to participate in the consensus process for transaction validation to earn block production rewards. In the PoS model, validators who attempt to manipulate transactions do so at the risk of losing their staked tokens. PoS builds on game theory concepts deployed in PoW to provide a more resource efficient consensus mechanism (*i.e.*, does not consume electricity for "mining" as in PoS). In the future, it is likely that different blockchains will choose consensus mechanism designs based on desired attributes in performance, scalability, and transaction finality, among other considerations.

4 Jamslevy, *EIP 867: Standardized Ethereum Recovery Proposals #866*, GitHub (Feb. 1, 2018), https://github.com/ethereum/EIPs/issues/866.

From a risk perspective, PoW and PoS systems are similar in that they can both be compromised through "51% attacks" where the consensus mechanism is manipulated by an actor seeking to process fraudulent transactions. To date, consideration of 51% attacks has focused on PoW consensus protocols as that consensus model is currently the most widely adopted. In order to better understand a 51% attack, we first provide a brief description of PoW and how the consensus mechanism functions.



At a high level, PoW is a cryptographic, mathematical puzzle that validators on a network aim to solve in order to win a block reward and the right to publish the next "block" of valid transactions to the network. The puzzle is solved by generating an arbitrary random input called a "nonce" (random inputs) into a one-way hash function with the aim of producing a fixed length value which meets a certain outcome condition. The likelihood of achieving the target outcome and solving the puzzle increases proportionally with a validator's ("miner") computational resources to produce nonces relative to the total population of computing resources producing nonces to solve the PoW algorithm ("hashpower"). The more rapidly a validator can produce nonces, the higher their probability of solving the PoW puzzle to publish the next block and win the block reward (currently 12.5 BTC on the Bitcoin network). Validators are also paid transaction fees which creates the incentive to collect all transactions to increase economic gain should the validator solve the puzzle and publish the next block. Validators are disincentivized from manipulating transactions because all transactions are shared on the network, creating a condition where an inaccurate transaction would be immediately identified to invalidate the block with the manipulated transaction(s). This consensus attack incurs a substantial opportunity cost to the malicious actor in the form of both forgone block rewards and wasted resources (electricity and computational resources).

A 51% attack against a PoW network requires the majority of a network's validating hashpower to perform a "double spend" attack by manipulating historical transactions to the malicious validators own economic advantage. This risk to PoW networks has been discussed frequently as hashpower has become more centralized. This is the result of the institutionalization of the mining industry and creation of mining pools, where miners combine their mining capacity to earn block rewards that are then distributed across the mining pool. Successful 51% attacks have been executed against smaller

PoW networks resulting in "double spends" and asset compromise. Most recently, the Ethereum Classic ("ETC") protocol fell victim to a 51% attack resulting in the compromise of more than 200,000 ETC valued in excess of $1 million USD at the time of the attack.[5]

PoS blockchains are also subject to the risk of a 51% attack where an individual validator or "staker" controls more than half the network assets and stakes more than 51% compromise the PoS consensus process. Discussion of 51% attacks on PoS networks continues to increase alongside adoption, both with regard to newly launched blockchains using PoS and older blockchains transitioning to PoS.

Regardless of the consensus mechanism, public blockchains validated through distributed consensus mechanisms are susceptible to distributed consensus compromise. The risks associated with an attack on a blockchain's consensus mechanism must be considered by practitioners interacting with native assets. In order to help address risks related to consensus mechanisms' compromise, practitioners in the ecosystem have developed blockchain threat monitoring solutions to help generate alerts when consensus attacks are attempted or executed. In closing, it is beneficial for practitioners interacting with digital assets on public blockchains to perform consensus attack modeling to understand the security posture of a given blockchain to inform business strategy, operations and risk management efforts.

3. CRITICALITY OF PRIVATE KEY MANAGEMENT

On a public blockchain, identities and the assets they own are not managed or tracked by a central institution. Identities are reflected on the network by the public key address of a defined "key pair." A key pair consists of a public key, visible to all network participants, and a cryptographically paired private key, which is kept secret and is required to execute transactions on behalf the related public key address. These key pairs are derived from asymmetric cryptographic algorithms which create a unique private key from each public key that is generated.[6] The combination of a private and public key pair composes a "wallet" as discussed within this piece.

Blockchain transactions processed using digital signatures are pseudonymous, meaning that every public key address ultimately correlates to an identity which is unknown. In this model, the counterparty's information is not recorded in on-chain transaction records, however, advanced analytics have been developed to try to unveil potential identities. Advances in zero-knowledge proof ("ZKP") cryptography and ring-signatures (*e.g.*, Z-cash, Monero, Dash) will further obfuscate transactional information including public wallets addresses from transaction details recorded on the ledger to further protect user privacy.

---

5 *See* Mark Nesbit, *Deep Chain Reorganization Detected on Ethereum Classic (ETC)*, The Coinbase Blog (Jan. 7, 2019), https://blog.coinbase.com/ethereum-classic-etc-is-currently-being-51-attacked-33be13ce32de.

6 It is worthwhile to note that advances in quantum computing will challenge existing approaches to asymmetric cryptography (including blockchain as well as any other use of such cryptography, which is commonly used); however, these considerations fall outside the scope of this discussion.

Private key management is an important consideration in permissioned blockchains; however, it is dramatically exacerbated when considering public blockchains and the factors discussed in Section A centering on the implications that a lack of central authorities has on asset recoverability. In public blockchains, the exposure of a private key fundamentally compromises all of the assets associated with the related public key wallet address. The need to protect private key material to "custody," or maintain ownership control of tokenized assets, has spurred a massive market with a diverse array of solutions targeting retail and institutional market segments.

From the retail perspective, investors in assets traded on public blockchains may choose to manage their own private keys in a "self-custody" model or opt to utilize a third-party wallet service or exchange. Investors choosing self-custody models should fully understand the risk they are responsible for holding the asset, with an appreciation that there is no path to pursue recourse in the case of asset compromise. As a result of self-custody risks, many users will engage the services of a wallet service, exchange, or brokerage platform to manage their private keys and effect transfers. This can be an option for asset owners to transfer the risk associated with private key management to a third-party to rely on the third-party's controls and process to mitigate cyber risks to private keys. This approach has resulted in high profile cyber and technology risk events, most recently and notably impacting QuadrigaCX, a Canadian exchange. QuadrigaCX was forced into bankruptcy after two unfortunate developments: QuadrigaCX CEO, Gerald Cotton, died with sole access to wallets containing cryptocurrency worth $137 million USD, affecting 115,000 customers; and, in the process of responding to Cotton's death, an additional $469,000 dollars was accidentally sent to the wallets that could not be accessed.[7] This risk event, while not directly cyber-related, highlights the criticality of key management and the implications for investors relying on third parties to manage risks related to cryptoasset custody.

"MAINTAINING THE CONFIDENTIALITY, INTEGRITY, AND AVAILABILITY OF PRIVATE KEYS REQUIRES THOUGHTFUL AND ROBUST CYBERSECURITY CONTROLS"

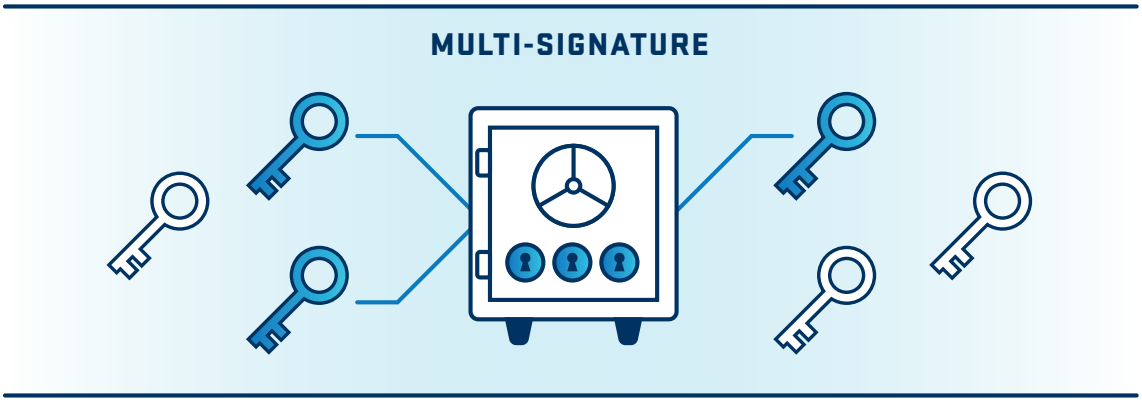
***— Erin English**, "Advancing Blockchain Cybersecurity"*

While retail and institutional custody models have similarities, there are differences in asset owners' and asset managers' requirements for risk management, security, and regulatory compliance in regard to both custodial and non-custodial models. To this point, there is strong competition across the

7 Colin Harper, *First QuadrigaCX Monitor Report: $460k in BTC "Inadvertently" Sent to Cold Wallet*, Bitcoin Magazine (Feb. 12, 2019), https://bitcoinmagazine.com/articles/first-qcx-monitor-report-460k-in-btc-inadvertently-sent-to-qcx-cold-wallet/.

institutional cryptoasset custody market, with a number of emergent business models and technology solutions being developed and adopted. Across these solutions, cyber risk is a critical consideration driving risk management and control innovation to help securely custody assets. As noted by Erin English in Advancing Blockchain Cybersecurity, "Maintaining the confidentiality, integrity, and availability of private keys requires thoughtful and robust cybersecurity controls."[8] These business process and control innovations have laid the foundation for best practice principles to effectively manage and custody private keys. While there are some key nuances, these principles and standards are largely derived from existing standards for cybersecurity and private key management.

Established approaches to cryptographic key management (*i.e.*, NIST 800-57, FIPS 140-2 Level 2/3) should be considered by practitioners providing custody products and services. The implementation of business based on established standards, security policies, operating procedures, and resiliency plans throughout key lifecycles is required to effectively protect private key material. Cyber risks should be considered through the key lifecycle from creation, initialization, distribution, operational utilization (active/inactive), and retirement.[9] These risks encourage practitioners to develop business processes to support private "key sharding," where a single private key is split into "shards," or requisite pieces, to decentralize the risk related to the private key. This approach renders each shard useless without assembling a defined number of the other shards. Key sharding has been implemented widely using Shamir's Secret Sharing ("SSS") to eliminate single points of failure where a private key can be compromised.



Similarly, the implementation of multi-signature wallets requiring two or more signers to transact can reduce single points of failure by requiring multiple users to sign transactions. This helps to increase the resiliency of control environments protecting private keys. Multi-signature wallet schemes may also integrate the use of independent, third-party signers who perform identity verification to authenticate transactions. In addition to key sharding and multi-signature schemes, research into the

8 English, Kim, and Nonaka, *supra* note 1.
9 Elaine Barker et al., Recommendation for Key management, Part 1: General (Revision 3), SP 800-57 Part 1 Rev. 3 (July 2012), https://csrc.nist.gov/publications/detail/sp/800-57-part-1/rev-3/archive/2012-07-10.

use of multi-party computation ("MPC") approaches, which allow multiple parties to compute a function over inputs while maintaining the privacy of the inputs, are being analyzed and incorporated to securely manage private keys. MPC approaches to key management have been deployed in Bring Your Own Key ("BYOK") models for public cloud infrastructure deployments to prevent key compromise by the cloud service provider ("CSP").[10] Similarly, MPC-based approaches to cryptographic key management can be integrated into custodial solutions to securely manage private keys to public wallets.

The focus on "crypto custody" has increased substantially through 2018 and 2019, largely due to persistent cyber-attacks on exchanges. While complex in practice and implementation, crypto custody simply refers to the business process and technology infrastructure designed for cryptoassets to securely store and managing the private keys. Crypto custody may be included in a broader suite of services offered by token trading platforms, as a standalone business model, or as a managed service. The technology environment supporting the given business performing the custody function is subject to traditional cyber risks which must be mitigated. These risks are present for all entities operating blockchain nodes, underlying infrastructure, and/or business processes interacting with the network and native assets.

In order to meet rising institutional demand and increasingly sophisticated service requirements, tiered custody models are frequently implemented to provide varying levels of security and availability to meet asset owner requirements. These approaches utilize strong network segmentation, resiliency by design and air-gapped physical vault storage using hardware security modules ("HSMs") to provide the highest levels of security against cyber risks. Regardless of the custody model and solution, established cyber frameworks (*i.e.*, NIST 800-53) and defense-in-depth principles to cybersecurity should be embraced to help securely manage private keys and protect assets hosted on public blockchains against cyber risks.[11]

4. PROTOCOL AND SMART CONTRACT VULNERABILITIES

Public blockchain protocols and smart contracts are software, and like all software they are susceptible to vulnerabilities. Traditional risks of software vulnerabilities must be considered and mitigated as public blockchains are launched and upgraded and as smart contracts are issued. For example, developer communities and ecosystem participants must perform rigorous software testing procedures and code-level reviews to manage these risks.

10 Tolga Acar, Mira Belenkey, Carl Ellison, and Lan Nguyen, Key Management in Distributed Systems, Microsoft (June 17, 2010), https://www.microsoft.com/en-us/research/wp-content/uploads/2010/06/Distributed-Key-Lifecycle-Management.pdf.

11 David W. Archer et al., *From Keys to Databases – Real-World Applications of Secure Multi-Party Computation*, 61 Comp. J. 1749, 1749 (2018), https://doi.org/10.1093/comjnl/bxy090.

At the protocol layer, the responsibility for testing is shared across the community. Developers and actors across the ecosystem have coalesced to develop software testing procedures and code reviews to help manage these risks. These testing procedures are often performed on "test nets" which are replicas of public blockchains where the software updates are deployed and tested. A compromise in a blockchain protocol is a critical risk consideration that must be regarded with the utmost importance by all related parties and reflected as such through integration into incident response policies to address a protocol layer breach.

This reality recently arose in the Bitcoin community with the identification of a protocol vulnerability (Bitcoin CVE 2018-17144[12]) that could have allowed a Denial-of Service driven "double-spend" attack. This scenario exposed a potentially existential risk to Bitcoin as the exploitation of this vulnerability could have deeply eroded trust in the protocol and asset itself. The community rallied to address the software flaw and it was ultimately remediated prior to exploitation. While this protocol risk was successfully addressed, participants quickly realized that the risk exposure extended across a number of other networks that had cloned the Bitcoin protocol.

While the risk of protocol vulnerabilities will always exist, academic institutions including MIT's Crypto Security Initiative are investing resources and performing security research to identify and patch blockchain protocol vulnerabilities. The institutions and organizations will play a critical role in guaranteeing the security and longevity of blockchain infrastructure and enabled assets.

While protocols serve as the foundational transaction layer, smart contracts provide applications that run on blockchains and, upon the occurrence of specified conditions, automatically execute functions.[13] Automated execution alleviates the need for intermediaries to manage terms and conditions between transacting counterparties, replacing them with programmed logic. Smart contracts can be deployed in a variety of use cases, however, the most frequently deployed use case to date has been to facilitate the issuance of tokens taking a variety of forms (*e.g.*, security, utility, commodity).

While a marvel of innovation, inherent risks to smart contracts exist that must be mitigated to prevent contract and asset compromise. Smart contracts issued on public blockchains are deployed to all nodes on the network, allowing all participants the ability to interact with the contract. The distribution of smart contracts across network participants increases the attack surface to include all network participants. This contrasts with permissioned blockchains where smart contracts are only exposed to the approved members of network limiting the attack surface to only known participants.

As with any software development, flaws and vulnerabilities in smart contract code have led to extensive risk events resulting in the compromise of millions of dollars of assets, most notably through

12 *CVE-2018-17144 Full Disclosure*, BitcoinCore (Sep. 20, 2018), https://bitcoincore.org/en/2018/09/20/notice/.
13 Chamber of Digital Commerce, Smart Contracts: Is the Law Ready? (Sept. 2018), https://digitalchamber.org/smart-contracts-whitepaper/.

the DAO hack, where 3.6 million ether was siphoned out of a smart contract through an exploited vulnerability (*i.e.*, a bug in the software).[14] In efforts to better understand the prevalence and scope of the issue, different academic studies have performed analytics over historically issued smart contracts. In one example, researchers from University College London (Ilya Sergey) and the School of Computing, NUS Singapore (Ivica Nikolic and Aashish Kolluri) analyzed nearly one million smart contracts deployed on the Ethereum blockchain concluding that thousands of issued contracts contain vulnerabilities that could lead to asset compromise.[15]

In recognition of the risks associated with smart contracts, industry participants and academic researchers continue to develop approaches to perform smart contract security audits and assessment. Frameworks have emerged and are evolving which can be adopted by practitioners to help ensure secure smart contract coding practices. For example, Consensys has released "a guide to smart contract security best practices" on GitHub.[16] In most use cases today, smart contracts undergo exhaustive third-party security audits and code reviews prior to issuance.

Alongside the propagation of smart contract security approaches, standards for specific smart contract use cases have emerged, namely token standards such as ERC20 in the Ethereum ecosystem. This standard has given entities issuing tokens on the Ethereum blockchain an option to rely on a standard contract structure. Participants gained increased comfort over security design due to the rigor of the community's review and approval process with this approach. In addition, standards enable more effective interoperability across tokens and underlying infrastructure. While token standards like ERC20 have increased security and interoperability, the structure lacks native capabilities to recover tokens in the event of a compromise.

To solve for this problem, developers have designed proprietary token structures to allow for asset recovery. These token structures include built-in mechanisms to facilitate the destruction and re-issuance of outstanding tokens in the event of a compromise. While a powerful feature for responding to theft, the ability to destroy tokens introduces centralization risk which could be exploited by the issuer or a malicious actor.

5. INACCURATE EXTERNAL DATA SOURCES

Smart contracts often rely on external data sources (sources outside the blockchain protocol) or "oracles" in order to execute conditional logic, introducing risk which much be considered and mitigated. In a simplistic model, oracle feeds introduce a central point of failure to smart contracts, an issue which has been called the "oracle problem."

14 David Siegel, *Understanding the DAO Attack*, Coindesk (June 25, 2016), http://www.coindesk.com/understanding-dao-hack-journalists/.
15 Ivica Nicolic et al., Finding the Greedy, Prodigal, and Suicidal Contracts at Scale, Cornell U. (Mar. 14, 2018), https://arxiv.org/abs/1802.06038.
16 Consensys Diligence, *Ethereum Smart Contract Security Best Practices*, GitHub, https://consensys.github.io/smart-contract-best-practices/ (Last accessed on May 30, 2019).

Smart contracts are commonly designed to execute based on external oracle data feeds. In this model, the risk of inaccurate external data being fed into a smart contract is critical. As with all technology systems, external data feeds and the supporting infrastructure must be effectively controlled and secured to protect against malicious actors targeting the smart contract. While the risk related to inaccurate external data sources is consistent across smart contract platforms, solutions are actively being designed to decentralize oracle data feed infrastructure.

C. CYBER POLICY AND REGULATORY CONSIDERATIONS

Tokenized assets on public blockchains are borderless by nature causing challenges for global regulatory authorities and complexity for practitioners in the space. Global regulators have been consistent in highlighting cybersecurity risks resulting in specific cybersecurity requirements for certain jurisdictions. In this section, we consider the U.S. cyber-related regulatory requirements at the Federal level, as well as the BitLicense cybersecurity requirements for entities operating within New York State.

1. JURISDICTIONAL CHALLENGES

The token economy is an emergent segment of the digital economy, defined by rapid innovation and an evolving risk landscape which must be managed by proactive adoption of established cybersecurity tools and guidance from governments and standards bodies. Participants in the token economy have worked diligently to rationalize positions across domestic regulators (*i.e.*, SEC, CFTC, FinCEN, IRS) and across international borders. While largely consistent with core intentions, challenges to compliance across multiple regulatory bodies can prove difficult.

2. SECURITY TOOLS AND MAPPING GUIDANCE

Security toolkits and mapping guidance assist organizations dealing with cybersecurity risks. To assist with control mapping efforts, tools and mapping guidance have been developed and released by standards bodies. Specifically, NIST has developed and open-sourced the Security Content Automation Protocol ("SCAP")[17] which can be readily adapted to automated security scans against control baselines (*i.e.*, NIST 800-53,[18] DISA STIG) and vulnerabilities to produce risk-rated reporting based on the severity of identified control gaps and vulnerabilities. This tool kit is managed by NIST and can be readily adopted as a component of organizational security practices to better understand coverage against a variety of control baselines and common enumerated vulnerabilities ("CVEs").

17 David Waltermire, Stephen Quinn, Harold Booth, Karen Scarfone, and Dragos Prisaca, *SP 800-126 Rev. 3: The Technical Specification for the Security Content Automation Protocol (SCAP)*, NIST (February 2018), https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-126r3.pdf.

18 Joint Task Force Transformation Initiative, *SP 800-53 Rev. 4: Security and Privacy Controls for Federal Information Systems and Organizations*, NIST (Apr. 2013), https://csrc.nist.gov/publications/detail/sp/800-53/rev-4/final.

Further, the manner in which a token is regulated will dictate certain cybersecurity requirements. For example, financial institutions must consider the Federal Financial Institutions Examination Council ("FFIEC") expectations for cybersecurity practices, including its guidance for cloud computing services and authentication of an internet banking environment when applicable.[19] These organizations should consider adopting the FFIEC Cybersecurity Assessment Tool to help identify cybersecurity risks and determine control environment maturity.

3. NEW YORK STATE BITLICENSE

New York State's BitLicense is a set of regulations administered and enforced by the New York State Department of Financial Services ("NYDFS") for virtual currency businesses serving New York residents. The regulation, Part 500 of Title 23 of the New York Code, requires companies with virtual currency operations in New York to obtain a license from the NYDFS and to comply with additional requirements as set forth in the regulations. The BitLicense, effective since March 2017, aims to protect customer information as well as the information systems by holding covered entities accountable for their cyber defense responsibilities, among other things.

The regulatory framework requires the implementation of a written cybersecurity program to include five core functions. Licensees must "establish and maintain an effective cybersecurity program to ensure the availability and functionality of their electronic systems and to protect those systems and any sensitive data stored on those systems from unauthorized access, use, or tampering." Furthermore, each licensee must:

- Designate a Chief Information Security Officer responsible for overseeing the cybersecurity program and policy;
- Comply with certain reporting and audit requirements relating to cybersecurity; and
- Ensure that applications follow written security standards and guidelines.

Similar to industry-leading frameworks such as ISO-27001, NIST SP 800-53r5, and NIST CSF, the BitLicense also requires licensees to establish and maintain a business continuity and disaster recovery ("BCDR") plan designed to ensure the availability and functionality of services in the event of an emergency or disruption to Licensee's normal business activities. The rules set forth minimum requirements for each BCDR plan such as annual testing and remediation activities.

19 *See* FFIEC, Outsourced Cloud Computing (July 10, 2012).

4. GDPR CYBER EVENT DISCLOSURE REQUIREMENTS

In May 2018, the European Union's General Data Privacy Regulations (GDPR) came into effect establishing specific expectations within Articles 32-34 for security and breach reporting. These domains have been covered extensively and will not be discussed in depth, however, given their applicability to entities within the token economy handling personal data of EU citizens, they warrant reference and inclusion within this narrative.

The security expectations established in GDPR require organizations to implement appropriate technology controls and procedures to ensure security commensurate with the entities' respective risk environment. The prevalence of cyber risk across actors in this space will establish foundational requirements including pseudonymization and encryption; ensuring confidentiality, integrity, availability, and resiliency of all systems; the ability to recover availability and access to personal data in the event of an incident; and the regular testing/evaluation of technological and operational controls to ensure security of data processing.

Further, GDPR has established requirements for breach documentation following any incident related to confidentiality, integrity, and/or availability. In addition, when a breach results in risk to the rights and freedoms of citizens, they must be reported to the Supervisory Authority ("SA") within 72 hours of breach identification. Specific reporting requirements must be included within the breach report to the SA.

Finally, we must acknowledge the clash between blockchain technology and its cryptographic immutability, and regulatory expectations regarding data deletion, namely GDPR Article 32's "Right to Be Forgotten." By design, transactions written to a blockchain are tamper-resistant. The data attributes of these transactions can, in some circumstances, contain identity information and/or cryptographic representations of an underlying identity (*i.e.*, public key address). If such information is written to a public blockchain, it cannot be removed. The application of the regulatory expectation to on-chain data has not been clearly defined, and, as such, it is a consideration that must be explored.[20]

20 *See Blockchain and the GDPR: Solutions for a Responsible Use of the Blockchain in the Context of Personal Data*, CNIL (Nov. 6, 2018), https://www.cnil.fr/en/blockchain-and-gdpr-solutions-responsible-use-blockchain-context-personal-data; *see also*, *Blockchain and the General Data Protection Regulation*, European Parliament (July 2019), https://www.europarl.europa.eu/RegData/etudes/STUD/2019/634445/EPRS_STU(2019)634445_EN.pdf.

D. GUIDELINES FOR ADVANCING CYBERSECURITY IN A TOKENIZED ECONOMY

In order to advance security across the ecosystem, practitioners and policymakers should consider the following guidance:

1 Practitioners interacting with digital assets on public blockchains should consider the challenges associated with asset recovery when developing policies, procedures, and technology infrastructure to develop robust preventative controls to prevent asset compromise. These policies may include the recommendations for "crypto custody" and key management, below.

2 Practitioners should develop policies, procedures, and technical infrastructure for crypto custody to securely manage digital assets throughout their lifecycle. These policies should limit the exposure of assets by balancing security and availability across tiered storage architectures to meet customer availability needs while limiting risk exposure to the assets. Practitioners may mitigate risk exposure by adopting key sharding techniques, multi-party computational approaches ("MPC"), multi-signature wallets, and third-party signers for identity validation/transaction authentication.

3 Practitioners must understand the risks to distributed consensus protocols by performing economic attack modeling to understand cost and likelihood of consensus mechanism attacks. These risks should inform business strategy and plans to integrate services with new public blockchains and assets.

4 Practitioners and participants choosing to self-custody their assets or to use a non-custodial solution must understand the implications of losing private keys and develop processes and approaches to mitigate these risks. These approaches may include utilizing specialized hardware for private key management, storing private keys in secure physical vaults, and creating resilience by backing up key replicas or recovery phrases in a geographically distributed and physically secure vault.

5 When using or building on public blockchains, protocol integrity and security must be guaranteed through robust testing procedures prior to production deployment through a "hard fork." Blockchain communities have taken and should continue to take conservative approaches to deploying software upgrades via hard forks to avoid inadvertently introducing new software vulnerabilities. Historically, the majority of protocol level testing procedures have been executed by developer communities; however, to the extent permitted by the relevant regulatory frameworks or conducted under the appropriate regulatory oversight, practitioners may consider investing resources into pre-launch testing procedures on "test nets" prior to adopting and deploying software upgrades.

6 Smart contract code is susceptible to vulnerabilities and requires a robust secure software development lifecycle including extensive testing and security auditing. As smart contracts (and associated code) become more complex, the risk of unintended outcomes for malicious attacks will increase. Practitioners must enforce comprehensive controls to carefully review, test, and monitor smart contract implementations to detect and prevent anomalies from being exploited. Smart contract code and ongoing outcomes should be continuously monitored to ensure that new vulnerabilities are identified and that outcomes are consistent with the contract's intended outcomes.

7 Practitioners must leverage established industry frameworks like NIST's Cybersecurity Framework ("CSF") to implement effective cybersecurity programs. In addition to the CSF, NIST provides the 800-53 control framework and accompanying automation tools for security monitoring (*e.g.*, Security Content Automation Protocol- SCAP: NIST SP 800-126) which can be adopted to help manage cyber risk.

8 Practitioners must carefully consider the laws of each jurisdiction before locating in or interacting with residents in those states/countries. They should also consider these requirements in the context of service providers that they may utilize when operating their business.

IV. CONCLUSION

Public blockchains have incredible potential to revolutionize business models and industries by enabling the internet of value to reduce costs for consumers and increasing transparency to ensure integrity within our economic, social, and environmental systems. In order to enable this future, practitioners and policymakers must continue collaboration to foster and develop best practices for cybersecurity within the crypto ecosystem. The guidelines set forth in this document aim to advance a dialogue around the cyber risks in the token economy and to encourage policymakers and practitioners to design standards for technical and business solutions to mitigate these risks.

Blockchain holds a unique position with regard to cyber risk and security. In many ways, blockchain can mitigate key cybersecurity risks inherent in the current internet structure by design using encryption and distributed computing models, while in other circumstances, the value of the assets hosted on blockchains make them a key target for malicious actors. Although it is beyond the scope of this report, it should be noted that cybersecurity extends beyond blockchain platforms to the devices that transact with them. The security models for e-commerce that rely on continuous observation and logging of data will not translate to the decentralized platforms of blockchain. To address this shortcoming, cybersecurity practitioners should consider leveraging blockchain implementations to capture the evidence of cybersecurity controls along with other transaction data to substantially increase the cybersecurity posture of any system and provide additional proof of compliance, at the transactional level, with applicable regulatory regimes.

The risk considerations and guidelines outlined in this chapter cannot be contemplated as afterthoughts to innovation. Effective cyber risk management and cybersecurity practices should be integrated into business models to ensure the security and longevity of blockchain technology to realize transformative, positive impacts to our economic, social, and environmental systems.

TOKEN ALLIANCE

CHAMBER OF DIGITAL COMMERCE

UNDERSTANDING DIGITAL TOKENS

Market Overviews and Trends in Token Project Fundraising Events

Prepared by the Token Alliance – an industry initiative of the Chamber of Digital Commerce

SECOND EDITION • AUGUST 2019

MARKET OVERVIEWS AND TRENDS IN TOKEN PROJECT FUNDRAISING EVENTS

The Chamber of Digital Commerce would like to thank Smith + Crown for their valuable contributions to the Token Alliance in the production of this report.

MATT CHWIERUT
Research Director

BRIAN LIO
Chief Executive Officer

LINDSAY NELSON
Research

BRANT DOWNES
Research

TABLE OF CONTENTS

II. METHODOLOGY

Measuring digital token project size is difficult. To do so, throughout this section, the term "digital token projects" or "token projects" includes all digital token fundraising events that: (i) entailed over $25,000 raised from project participants; (ii) involved the sale of digital tokens (as opposed to equity or debt); and (iii) did not return these raised funds. Amounts raised are valued according to average daily exchange rates on the date the fundraising event closed. Also, for purposes of this section, fundraising events for digital tokens are defined to take place regardless of whether tokens are distributed immediately or are promised to be delivered to project participants in the future (and have yet to be created, like Filecoin). The scope of analyses in this section thus includes all "presales," "private sales," "pre-ICOs," and so-called "Initial Coin Offerings" or "ICOs," as well as both meta-tokens on Ethereum (most of which are based on the ERC-20 standard), meta-tokens on other blockchains, and base tokens in fundamental protocols. Any of such events will more generally be referred to as a "token project fundraising event." The analyses set forth below also include "temporary tokens" that are intended to be redeemable for future tokens. Some data may be missing or subject to future revision, and fundraising events occurring more than 30 days apart are treated as separate.

III. INTRODUCTION

The year 2018 saw a significant decline, as the year progressed, in both the volume and the amount of funds raised through token project fundraising events, often referred to as "ICOs" or "token sales." The slowdown in token-based fundraising mirrored the overall bear market for cryptoassets throughout 2018 and into Q1 2019, and was arguably the dominant industry narrative in popular media. Despite this trend, the resilience of project fundraising efforts throughout the year, including a reemerging role for traditional venture funding, illustrated how backing continued to be available for strong projects across the space.

The fullest accounting of 2018 market activity likely incorporates a range of factors, some of which may only be discernible with greater distance. What is clear is that despite the overarching downward market trend, a closer look at 2018 shows a number of significant developments influencing token project fundraising, including:

- Token project fundraising events outperformed 2017 in terms of overall amounts raised and quantity completed when considered holistically. Fundraising continued for blockchain-based projects throughout the year, though approaches shifted toward more traditional fundraising vehicles.
- Virtually every part of the blockchain industry saw development, arguably by more qualified and serious teams with the commitment and means to weather the market downturn. The information, finance, and media industries experienced the most concentrated activity.
- Projects focusing on developing infrastructure solutions and core blockchain platforms attracted significant funding, working toward opportunities to underpin the future of blockchain technology.

These observations remind us to consistently challenge our definitions of success as the industry evolves. While quantity of fundraising, number of participating projects, and market activity were front and center as measures of industry success in 2017, 2018's progress can be found in the quality of projects continuing foundational work and the elimination of low quality actors. While Q1 2019 experienced new lows in terms of amounts raised through token-based fundraising, March and April trended slightly upward with renewed activity. May 2019 saw a sizeable increase in token-based fundraising, with virtually all of this increase attributable to Bitfinex's $1 billion raise, suggesting an increase of similar magnitude may not prove to be an enduring trend.

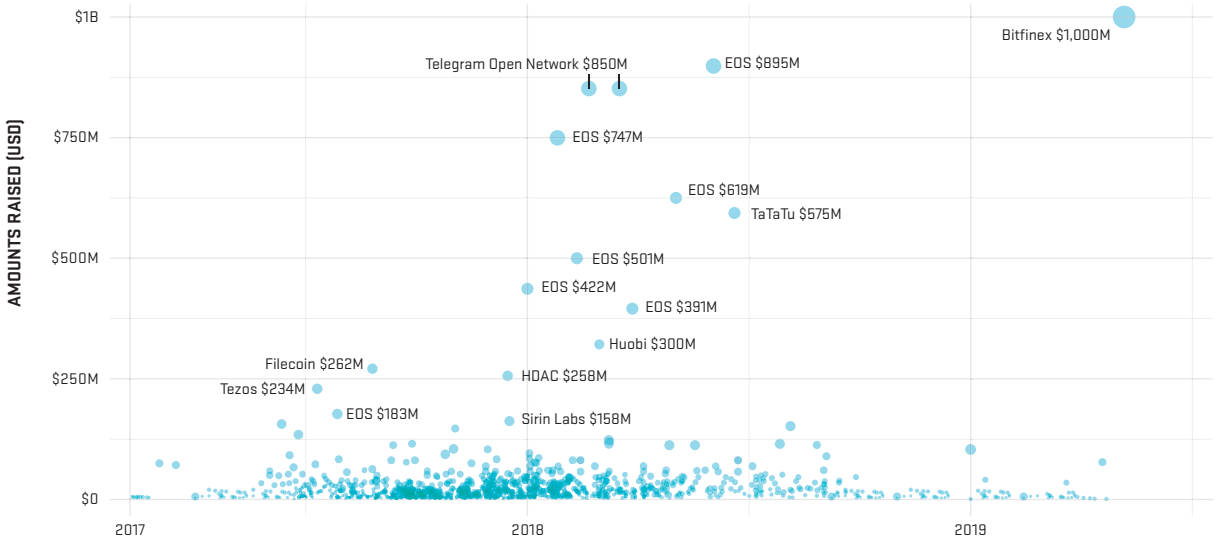
IV. TRENDS IN TOKEN PROJECT FUNDRAISING EVENTS: 2013-PRESENT

Figure 1 demonstrates a high-level view of the token project fundraising landscape. Both size and volume of project fundraising events tapered off over the course of 2018 and into 2019 with raises over $150 million disappearing after Q2 2018, prior to Bitfinex's raise.

FIGURE 1

TOKEN PROJECT FUNDRAISING LANDSCAPE 2017- MAY 2019

SMITH+CROWN



Note: Token project fundraising events above $150 Million are labeled.

Note: Token project fundraising includes all token projects that raised over $25,000 and did not return funds raised to participants. Amounts raised are valued according to average daily exchange rates on the date the fundraising closed. Rounds for the same project that are separated by more than 30 days are treated as separate fundraising events. EOS's ongoing fundraising events are valued according to the total raised during each period and grouped into monthly amounts with each month being treated as a separate "fundraising event" and, thus, are highlighted in a different color. Some data may be missing or subject to future revision.

TOTAL AMOUNTS RAISED IN TOKEN PROJECT FUNDRAISING EVENTS

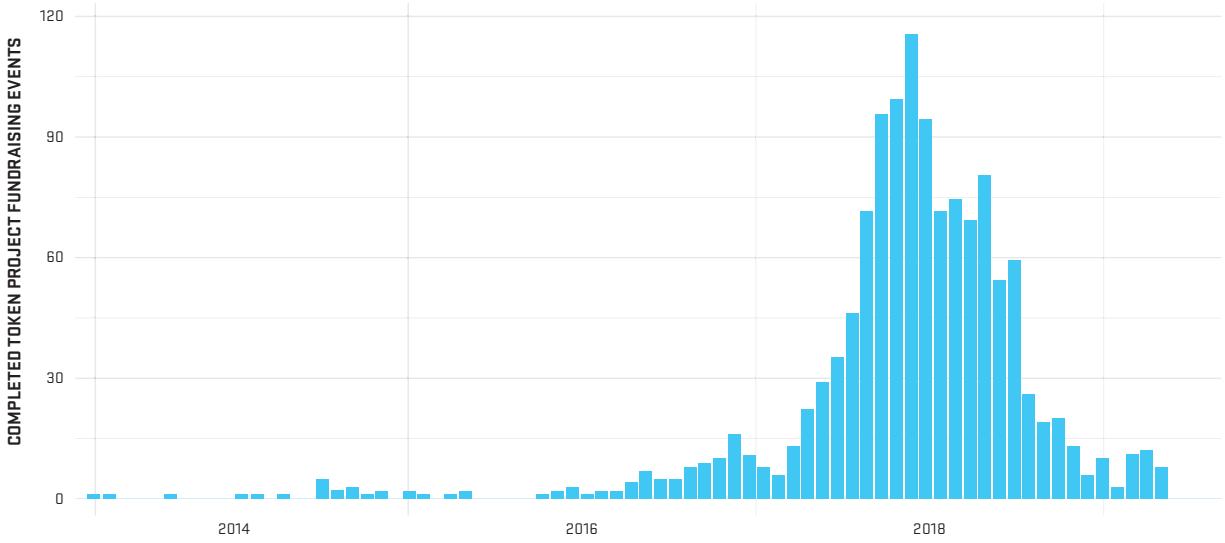
From January 2017 through December 2018, more than 1,100 token project fundraising events raised over $21.52 billion and, despite the recent market slowdown, $13.7 billion was raised in 575 fundraising events in 2018 alone. Relative to token project fundraising activity in 2017, where over 549 events raised $7.3 billion, 2018 saw an overall increase in both total number of fundraising events and amounts raised, despite the front-loaded nature of these events into the year's earlier months and the generally descending monthly trend in both number of fundraising events and amounts raised over the course of the year. $1.3 billion has been raised from 54 token fundraising events from January through May 2019, with Bitfinex's outsized raise accounting for $1 billion of that amount. While that represents a substantial sum, the ongoing declining trend in both average and median token fundraising events amounts remains concerning.

FIGURE 2

COMPLETED TOKEN PROJECT FUNDRAISING EVENTS

MONTHLY, JAN 2014 - MAY 2019

SMITH+CROWN



Note: Token project fundraising includes all token projects that raised over $25,000 and did not return funds raised to participants. Amounts raised are valued according to average daily exchange rates on the date the fundraising closed. EOS's ongoing raise is valued according to the total raised during each auction period and grouped into monthly amounts. Rounds for the same project that are separated by more than 30 days are treated as separate fundraising events. Some data may be missing or subject to future revision.

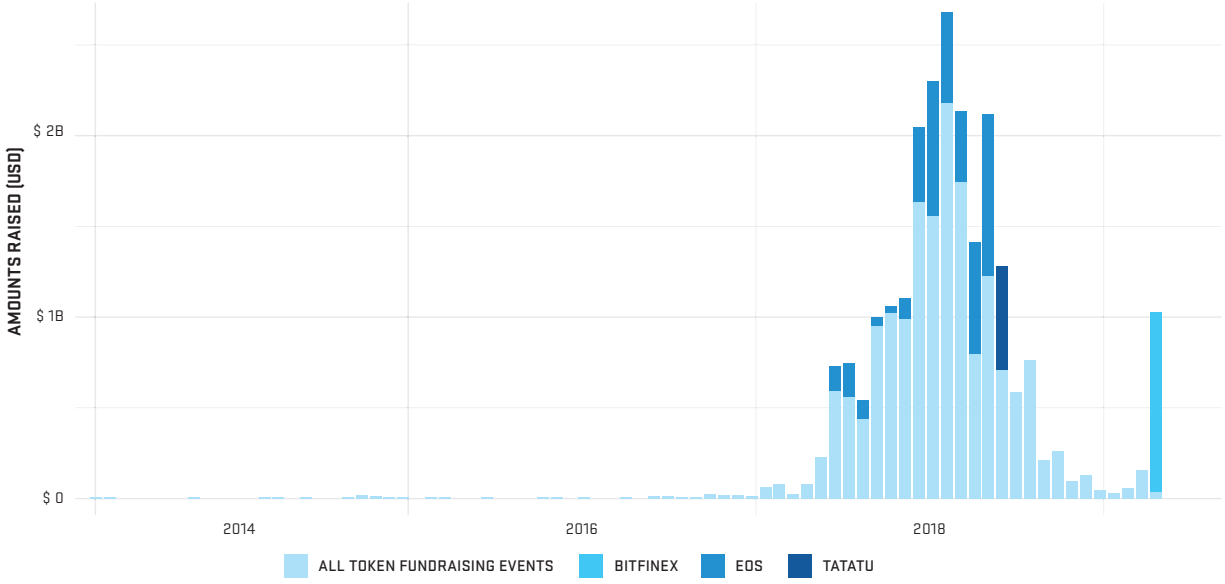
While the overall amount raised through token fundraising events through May 2019 is more than $22.8 billion, when those that raised more than $500 million are excluded, that figure declines considerably, to $16.8 billion. Similarly, excluding the single largest raise thus far in 2019 reduces the total amount raised from $1.3 billion to $359.2 million. This reinforces how media reports of headline numbers are frequently skewed by a focus on a small number of outsized fundraising events. Figure 3 illustrates how a significant bias towards the largest fundraising events has in many ways defined these markets, a perspective that has unfortunately lent itself to overlooking a large number of strong projects completing more modest fundraising events in support of fundamentally strong projects. While the absence of these largest fundraising events in the second half of 2018 is unsurprisingly the largest factor in the slowdown of the overall token fundraising market during this period, this focus on the largest raises also lends itself to an underestimation of the extent of activities and fundraisings still occurring.

FIGURE 3

FUNDS RAISED TO SUPPORT TOKEN PROJECTS

MONTHLY, JAN 2013 - MAY 2019

SMITH+CROWN



Note: Token project fundraising includes all token projects that raised over $25,000 and did not return funds raised to participants. Amounts raised are valued according to average daily exchange rates on the date the fundraising closed. EOS's ongoing raise is valued according to the total raised during each auction period and grouped into monthly amounts. Rounds for the same project that are separated by more than 30 days are treated as separate fundraising events. Some data may be missing or subject to future revision.

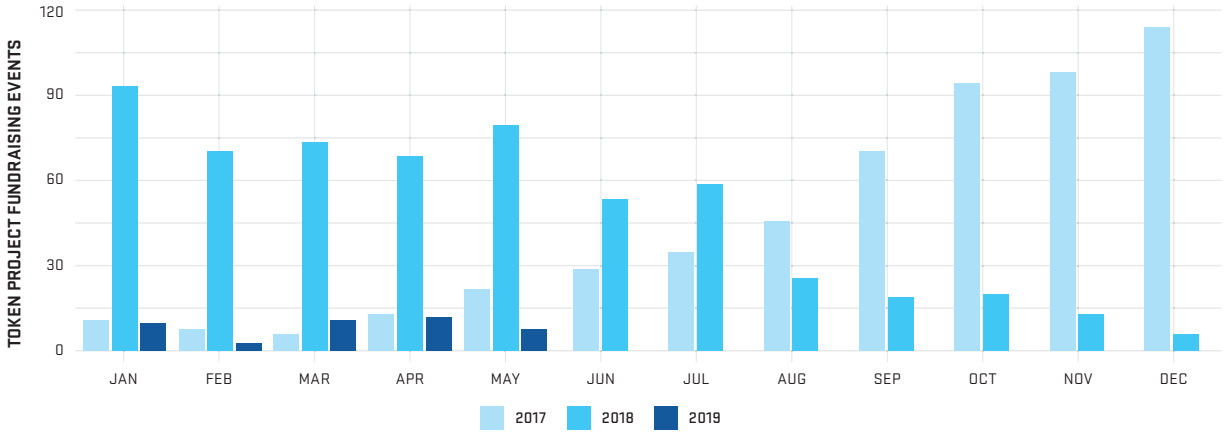
Figures 4 and 5, below, illustrate how both the number of token fundraising events and amounts raised have fallen substantially below prior-year comparisons.

FIGURE 4

TOKEN PROJECT FUNDRAISING EVENTS

MONTHLY, JAN 2017 - MAY 2019

SMITH+CROWN



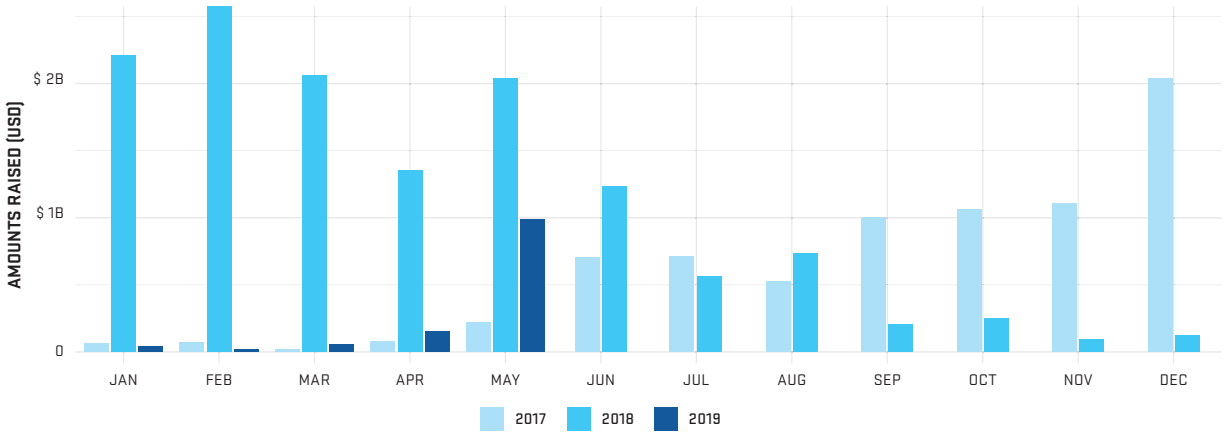
Note: Token project fundraising includes all token projects that raised over $25,000 and did not return funds raised to participants. Amounts raised are valued according to average daily exchange rates on the date the fundraising closed. EOS's ongoing raise is valued according to the total raised during each auction period and grouped into monthly amounts. Rounds for the same project that are separated by more than 30 days are treated as separate fundraising events. Some data may be missing or subject to future revision.

FIGURE 5

FUNDS RAISED TO SUPPORT TOKEN PROJECTS

MONTHLY, JAN 2017 - MAY 2019

SMITH+CROWN



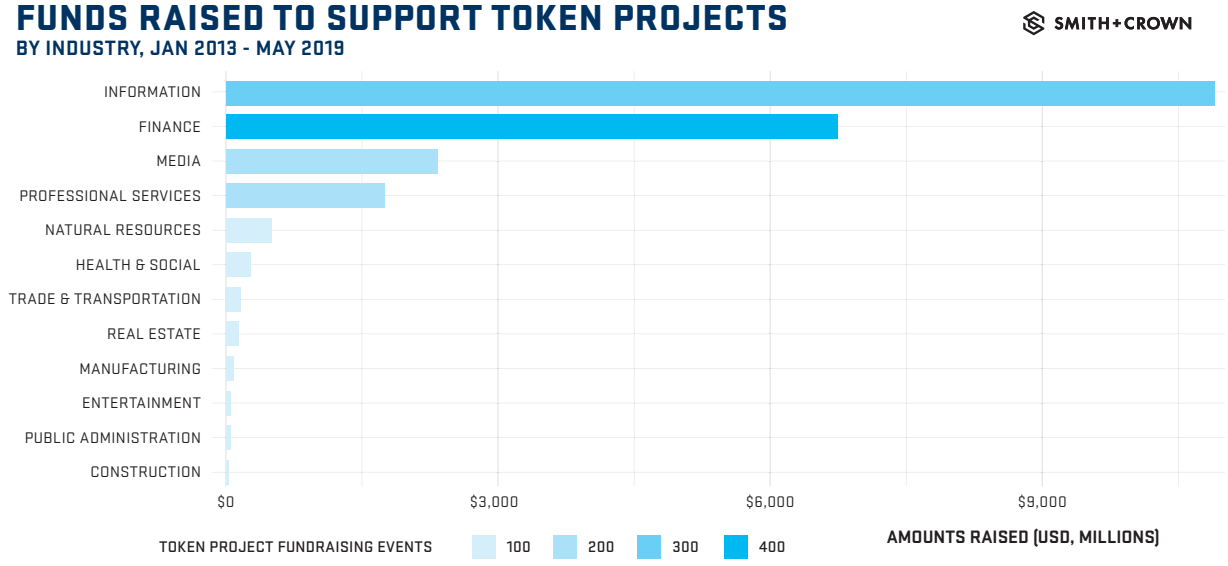
Note: Token project fundraising includes all token projects that raised over $25,000 and did not return funds raised to participants. Amounts raised are valued according to average daily exchange rates on the date the fundraising closed. EOS's ongoing raise is valued according to the total raised during each auction period and grouped into monthly amounts. Rounds for the same project that are separated by more than 30 days are treated as separate fundraising events. Some data may be missing or subject to future revision.

Looking across industries, both token fundraising event volumes and amounts raised remain concentrated across a few key industries. Among these were the information and finance industries with media and professional services trailing behind, as highlighted in Figure 6. The information service industry, which includes the blockchain protocol and smart contract platform sectors, received the most activity and funding. This suggests the market remains in a long-term, infrastructurally-orientated state, focused on the foundational layers for the next generation of products and services, such as smart contract platforms, exchanges, and other financial infrastructure.

FIGURE 6

FUNDS RAISED TO SUPPORT TOKEN PROJECTS

BY INDUSTRY, JAN 2013 - MAY 2019



Note: Color intensity of bar corresponds to number of token project fundraising events within industry.

Note: Token project fundraising includes all token projects that raised over $25,000 and did not return funds raised to participants. Amounts raised are valued according to average daily exchange rates on the date the fundraising closed. EOS's ongoing raise is valued according to the total raised during each auction period and grouped into monthly amounts. Rounds for the same project that are separated by more than 30 days are treated as separate fundraising events. Some data may be missing or subject to future revision.

The different industries are briefly described below:

Information - Smart contract platforms, distributed computing, data storage, and data analytics.

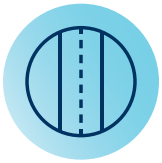
Finance - Payments systems, distributed trading platforms, and distributed prediction markets.

Media - Gaming, messaging, entertainment, and social networks.

Professional Services - Advertising/marketing, accounting, identity management, legal services, and loyalty rewards.

Natural Resources - Energy, agriculture, and precious metals.

Health & Social - Medical services, non-profits, social services, and education.



Trade & Transportation - Personal transportation services, supply chain management, and transportation of goods.

Real Estate - Commercial, residential, property management, and real estate investment funds.

Entertainment - Film, art, music, and other fine arts.

Public Administration - Voting mechanisms, record keeping, and governance platforms.

Manufacturing - Hardware devices and other manufacturing enterprises.

Note: Smith + Crown has considered this issue carefully in developing an estimation of blockchain-related activity across a range of industries and sectors and has implemented the following approach to industry classification. Projects are classified according to their target market, that is, whichever industry in which they are hoping to compete or which they are trying to disrupt. If the project's market is industry-agnostic, classify according to the product. For example, if it is a general purpose payment system, it operates in payment-processing sector. In addition, there are several new sectors that are specific to the blockchain industry, including smart contract platforms and prediction markets by which projects can be classified. Finally, the NAICS code industry system is used as a master category system for industries and newly emerging sectors.

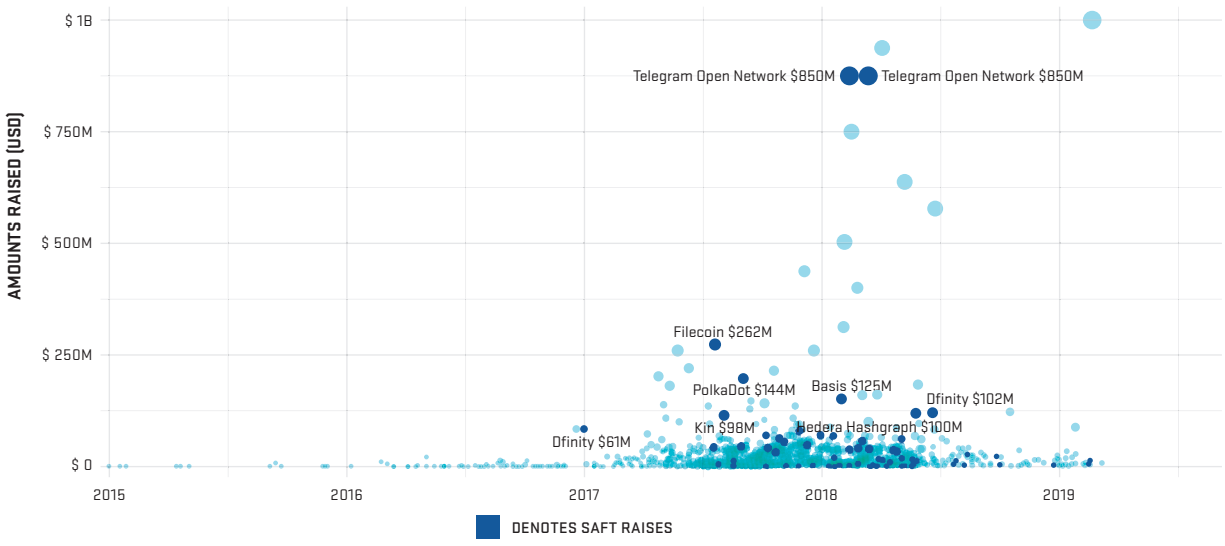
SHIFTS IN TOKEN PROJECT FUNDRAISING VEHICLES

The year 2017 saw the introduction of the **SAFT instrument (Simple Agreement for Future Tokens)** used to raise money for token projects. While the law firm Cooley refined the concept and launched **the original whitepaper** alongside collaborators Protocol Labs, AngelList, and CoinList, numerous SAFT-like instruments have been developed and deployed by other entities. Figure 7 shows activity across the broader token fundraising market with raises conducted under SAFT instruments identified in navy. Most SAFTs are restricted to accredited investors and many are also increasingly registering with national regulatory bodies under official fundraising regimes, most commonly Regulation D in the United States. Despite initial optimism that SAFT raises would present a path for avoiding compliance pitfalls and securities regulations for token-based fundraising, the vehicle appears not to have found widespread use. That is, it did not appear to take over as the predominant fundraising vehicle for token projects. The graph below illustrates both the limited number of raises conducted as SAFTs and how their pace of issuance has declined throughout Q3 2018. A reversal of this trend may take place if and when regulatory clarity around token project fundraising increases.

FIGURE 7

TOKEN PROJECT FUNDRAISING EVENTS VIA SAFT

JAN 2015 - MAY 2019



Source: Smith + Crown data; EDGAR database; Smith + Crown analysis.

Note: Token project fundraising includes all token projects that raised over $25,000 and did not return funds raised to participants. Amounts raised are valued according to average daily exchange rates on the date the fundraising closed. EOS's ongoing raise is valued according to the total raised during each auction period and grouped into monthly amounts. Rounds for the same project that are separated by more than 30 days are treated as separate fundraising events. Some data may be missing or subject to future revision.

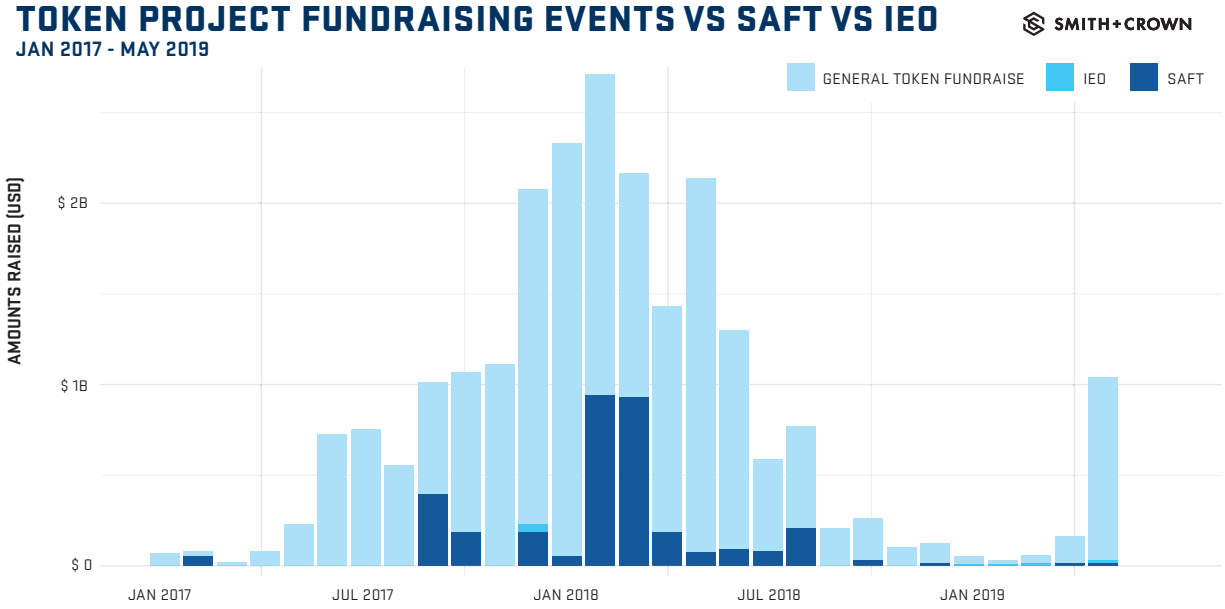
Figure 8 further reinforces this conclusion: while funds raised by traditional token fundraising events continued to decline throughout 2018, raises structured as SAFTs or expressly selling security tokens had yet to begin to fill the gap. Token fundraising events have begun to reemerge in 2019 with a small subset representing a new style of token fundraising event, dubbed an "Initial Exchange Offering" or "IEO."

While IEO's have no formal definition, they loosely refer to token fundraising events facilitated by cryptocurrency exchanges in exchange for service fees, tokens, or other compensation from the project raising funds. The concept of an IEO first emerged when the Binance exchange began hosting the token sales of blockchain-based projects in 2017, namely, those of Gifto and Bread. The term "IEO" was not intentionally coined by Binance but rather took on a colloquial meaning in the crypto community. Other exchanges began participating in the trend around early 2019. It's important to note that collecting and reporting on IEO data is difficult due to inconsistent, contradictory, or absent data. Because of this, Smith + Crown has taken a conservative approach to classifying raises as "IEO." Figure 8 represents only the 17 all-time token fundraising events that we feel sufficiently meet the definition of the term IEO and have externally verifiable funding data. These 17 IEOs have collectively raised $90.2 million since they first emerged and, excluding the 2 IEOs that took place in 2017, shows that 15 IEOs have raised a total of $54.2 million from January through May 2019. While important to highlight as an emerging fundraising trend, Figure 8 shows that IEOs have only slowly gained traction in terms of number of raises and amounts raised and, therefore, have yet to make a meaningful impact on the overall token based fundraising event landscape.

FIGURE 8

TOKEN PROJECT FUNDRAISING EVENTS VS SAFT VS IEO

JAN 2017 - MAY 2019



Note: Token project fundraising includes all token projects that raised over $25,000 and did not return funds raised to participants. Amounts raised are valued according to average daily exchange rates on the date the fundraising closed. EOS's ongoing raise is valued according to the total raised during each auction period and grouped into monthly amounts. Rounds for the same project that are separated by more than 30 days are treated as separate fundraising events. Some data may be missing or subject to future revision.

REEMERGENCE OF EQUITY-BASED FUNDRAISING

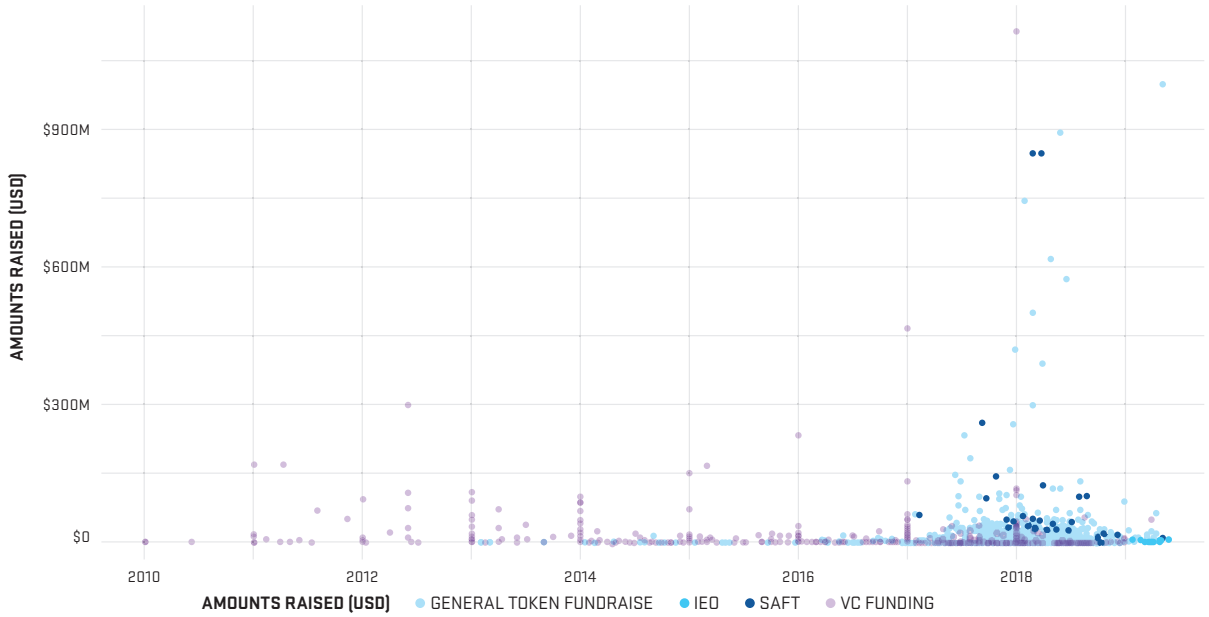
Another important fundraising trend for cryptocurrency and blockchain projects, the importance of which both complements and is reinforced by the decline in general token project fundraising and SAFT raises, has been the emerging importance of venture capital funding throughout 2018, particularly the latter half of the year. While this trend has taken many particular forms, including debt and convertible notes, most prominent has been the traditional venture capital approach involving the sale of project equity. While many mentions of this trend during 2018 saw it as a shift away from token-based fundraising, variously attributed to a host of reasons, and towards venture funding, Figure 8 provides a somewhat different perspective. By comparing project fundraisings on a longer-term basis where token raises – with SAFT sales broken out as a unique sub-sector – appear alongside of venture raises, what emerges is a clear sense of how venture raises have traditionally been the dominant form of fundraising in the industry. Only during the mid-2017 to mid-2018 period did token-based raises overtake equity-focused venture raises. Given that cumulative token-based fundraising accounted for more than twice the amount raised by venture funding, $18 billion versus $7 billion, it is understandable how attention has focused on token-based fundraising. From a longer-term perspective, however, there have been more venture raises in the space and over a longer period than token-based fundraising events. While several interpretations may be drawn from these observations,

this extended perspective upon the project fundraising space suggests the shift towards equity raises with venture capital firms that marked the latter half of 2018 might be more a return to traditional practices than the novel shift it is often described as being.

FIGURE 9

FUNDS RAISED TO SUPPORT TOKEN PROJECTS, BY RAISE TYPE, JAN 2011 - MAY 2019

SMITH+CROWN



Source: Smith + Crown data; Crunchbase data; Smith + Crown analysis.

Note: Token project fundraising includes all token projects that raised over $25,000 and did not return funds raised to participants. Amounts raised are valued according to average daily exchange rates on the date the fundraising closed. EOS's ongoing raise is valued according to the total raised during each auction period and grouped into monthly amounts. Rounds for the same project that are separated by more than 30 days are treated as separate fundraising events. Some data may be missing or subject to future revision.

V. CONCLUSION

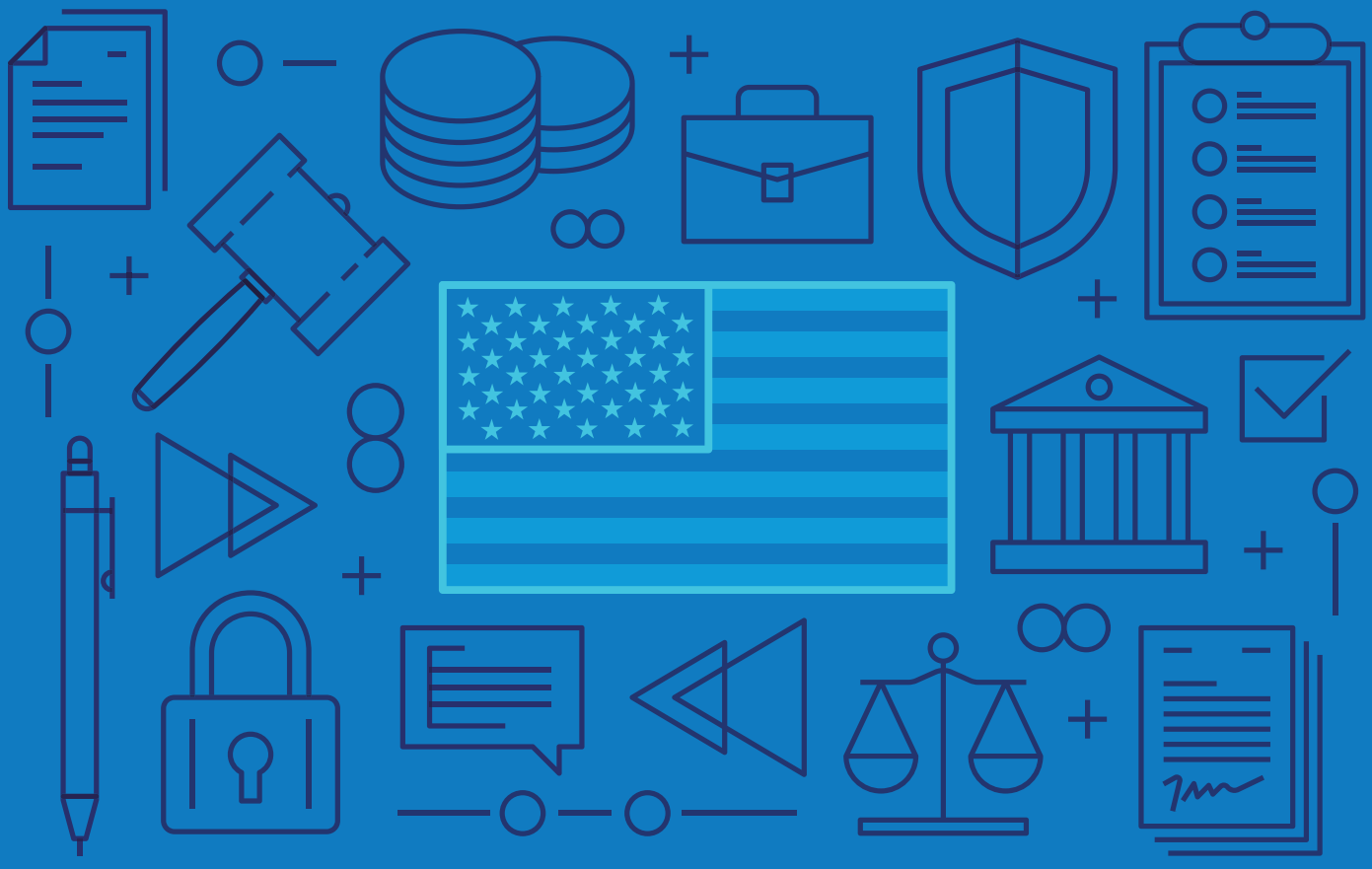
Overall, while the digestion of gains made throughout 2017 has been a widely recognized theme of 2018, virtually every aspect of the cryptoasset space saw ongoing development, considerable amounts of which were supported by equity raises and venture capital funding. This suggests that a range of actors – from start-ups, to name brands, established companies, investment firms, and even governments – remain committed to erecting the infrastructure for a larger, farther-reaching, and more impactful cryptoasset space. How the funding space continues to evolve and the corresponding implications warrant close observation given their profound impact on development of the space.

TOKEN ALLIANCE

CHAMBER OF DIGITAL COMMERCE

UNDERSTANDING DIGITAL TOKENS

Legal Landscapes Governing Digital Tokens in the United States

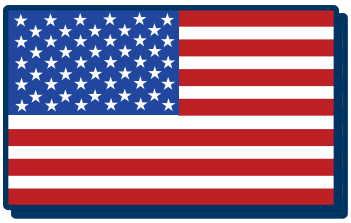


Prepared by the Token Alliance – an industry initiative of the Chamber of Digital Commerce

FIRST EDITION • JULY 2018

II. PART 1: REGULATORY OVERVIEW OF DIGITAL TOKEN MARKETS

SECTION 1: UNITED STATES



I. INTRODUCTION

This Section provides an overview of United States rules and regulations applicable to digital tokens, primarily focusing on the distinct regulatory frameworks for digital tokens that are commodities, versus those that are securities. In doing so, this Section sets forth criteria used by regulators to assess whether a digital token meets either regulatory classification. It also provides a summary of various regulatory considerations related to consumer protection, state money transmission laws, and federal money laundering rules. Subsequent parts present overviews of the regulatory environment in Canada, the United Kingdom, Australia, and Gibraltar for digital tokens.

In the regulatory sense, digital tokens largely, though not exclusively, fall into two broad categories: 1) commodities; and 2) tokenized securities. Each category brings about important regulatory considerations, although some digital tokens likely fall into neither regulatory category.

United States Securities and Exchange Commission ("SEC") Chairman Jay Clayton has stated publicly that he does not view virtual currencies to be securities[1] and SEC Director of Corporation Finance William Hinman has stated publicly that bitcoin and ether are not securities;[2] however, to date, the SEC has not formally determined that virtual currencies are not securities. Meanwhile, the United States Commodity Futures Trading Commission ("CFTC") has determined that virtual currencies like bitcoin are commodities,[3] and at least one court has upheld that view.[4] Tokenized securities, like other securities,

1 Interview by Bob Pisani with Jay Clayton, Chairman, U.S. Sec. and Exch. Comm'n, in New York, N.Y. (June 6, 2018).
2 William Hinman, Digital Asset Transactions: When Howey Met Gary (Plastic): Remarks at the Yahoo! Finance All Markets Summit: Crypto (June 14, 2018), https://www.sec.gov/news/speech/speech-hinman-061418.
3 *See infra* note 8 and accompanying text.
4 *Commodity Futures Trading Comm'n v. McDonnell*, No. 1:18-cv-00361-JBW-RLM, slip op. (E.D.N.Y. Mar. 6, 2018), https://www.cftc.gov/

are subject to SEC jurisdiction, but are different than other securities in that they may apply blockchain technology to raise funds, track ownership, and deliver value to owners. "Utility tokens" (also known as "app-coins") – which, as SEC Commissioner Hester Peirce recently remarked, can "function as a means of executing a transaction, as a way to get access to a product or service or participate in a community, or in any number of ways that have yet to be dreamed up"[5] – may be commodities, or may be neither securities nor commodities. Tokens that are neither securities nor commodities are presumably regulated under the Federal Trade Commission's ("FTC") anti-fraud and other consumer protection authorities, as well as other regulatory regimes. Unfortunately, some distributions of tokenized securities have characterized or claimed the offered assets as "utility tokens," to steer clear of securities-registration requirements. These tokens are not "utility tokens."

Broadly, state attorneys general and the FTC have the authority within their jurisdictions to enforce a variety of anti-fraud and consumer protection laws in markets for all types of digital tokens, while the United States Treasury Department has a range of anti-money laundering and sanctions enforcement powers. Additionally, markets for digital tokens are subject to a number of tax law implications.

II. LEGAL CLASSIFICATIONS & RELATED REGULATORY CONSIDERATIONS

A. VIRTUAL CURRENCIES AND MANY APP-COINS – COMMODITIES, NOT SECURITIES

The term "commodity," as defined in the Commodity Exchange Act ("CEA"), is very broad, and includes "all services, rights, and interests… in which contracts for future delivery are presently or in the future dealt in."[6] Only onions and box office receipts are expressly excluded from the definition. The CFTC, in prior enforcement actions, has determined that "bitcoin and other virtual currencies" are a type of "commodity,"[7] and as mentioned above, a federal court has likewise ruled that the term "'commodity' encompasses virtual currency both in economic function and in the language of the statute."[8] While no statutory definition for the term virtual currency exists, in December 2017, the CFTC stated in a proposed regulatory interpretation that it interprets the terms "virtual currency" and "digital currency" to encompass:

- any digital representation of value (a "digital asset") that functions as a medium of exchange, and
- any other digital unit of account that:

sites/default/files/idc/groups/public/@lrenforcementactions/documents/legalpleading/enfcoindroporder030618.pdf.

5 Hester Peirce, Beaches and Bitcoin: Remarks before the Medici Conference (May 2, 2018), https://www.sec.gov/news/speech/speech-peirce-050218.

6 The term "commodity" is defined in the Commodity Exchange Act ("CEA") as "wheat, cotton, rice, corn, oats, barley, rye, flaxseed, grain sorghums, mill feeds, butter, eggs, Solanum tuberosum (Irish potatoes), wool, wool tops, fats and oils (including lard, tallow, cottonseed oil, peanut oil, soybean oil, and all other fats and oils), cottonseed meal, cottonseed, peanuts, soybeans, soybean meal, livestock, livestock products, and frozen concentrated orange juice, and all other goods and articles, except onions (as provided by section 13–1 of this title) and motion picture box office receipts (or any index, measure, value, or data related to such receipts), and all services, rights, and interests (except motion picture box office receipts, or any index, measure, value or data related to such receipts) in which contracts for future delivery are presently or in the future dealt in."

7 See In the Matter of: Coinflip, Inc., d/b/a Derivabit, and Francisco Riordan, CFTC Docket No. 15-29 (Sep. 17, 2015), 3, http://www.cftc.gov/idc/groups/public/@lrenforcementactions/documents/legalpleading/enfcoinfliprorder09172015.pdf.

8 CFTC v. McDonnell, *supra* note 6.

- is used as a form of a currency (i.e., transferred from one party to another as a medium of exchange);
- may be manifested through units, tokens, or coins, among other things; and
- may be distributed by way of digital "smart contracts," among other structures.[9]

On the other hand, bitcoin and other similarly designed digital tokens do not appear to be securities, as that term has been interpreted under the United States Supreme Court's holding in *SEC v. W.J. Howey Co.*,[10] subject to SEC regulation. Indeed, SEC Chairman Jay Clayton recently noted that bitcoin "has been determined by most people to not be a security."[11] His colleague SEC Commissioner Hester Peirce similarly remarked in May 2018 that she is not yet "willing to make a blanket statement that everything other than bitcoin is a security,"[12] and in April 2017, SEC's Division of Corporate Finance Director Bill Hinman noted that "it is certainly possible that there are tokens that would not have the hallmarks of a security."[13] Regarding the features of non-security digital tokens, Mr. Hinman noted that such tokens would include those for which the token holder is buying a token "for its utility rather than investment, especially if it's a decentralized network in which it's used with no central actors." The SEC's recent interpretations of the *Howey* Test with regards to digital tokens, and regulatory considerations associated with tokenized securities, are described in greater detail below.

BRIAN QUINTENZ
CFTC COMMISSIONER

Clearly, the range of digital tokens that are not deemed by United States regulators to be securities may be quite broad. For example, Filecoin is a so-called "utility token" according to CFTC Commissioner Brian Quintenz.[14] Commissioner Quintenz recently drew a distinction between virtual currencies and "utility tokens" in a speech before the Chamber of Digital Commerce,[15] and in more recent remarks, noted that a motivation for creating digital token markets "is to utilize the transferability of tokens to create a secondary market for… non-tangible things."[16] He also expressed his belief that "[e]mpowering a secondary market's price discovery and valuation functions for products that were previously untransferable – such as extra storage space on a home computer – is a fascinating development."

9 Retail Commodity Transactions Involving Virtual Currency, 82 Fed. Reg. 60,335 (Dec. 20, 2017) (hereinafter "Actual Delivery Proposed Interpretation").
10 SEC v. W.J. Howey Co., 328 U.S. 293, 299 (1946).
11 *FY 2019 U.S. Securities and Exchange Commission: Hearing Before the Subcomm. on Fin. Services and General Government of the H. Comm. on Appropriations*, 115th Cong. (2018) (statement of Jay Clayton, Chairman, U.S. Sec. and Exch. Comm'n).
12 Kia Kokalitcheva, *SEC Commissioner Won't Declare All Tokens Are "Securities,"* AXIOS (May 3, 2018), https://www.axios.com/sec-crypto-securities-1525340196-82046d9e-a0ac-47c2-ae95-16ddae8a2b63.html (quoting SEC Comm'r Hester Peirce's speech delivered on May 2, 2018, Remarks at the Medici Conference).
13 *Oversight of the SEC's Division of Corporate Finance: Hearing Before the Subcomm. on Capital Markets, Securities, and Investment of the H. Comm. on Fin. Services,* 115th Cong. (2018) (statement of William Hinman, Director of the Division of Corporation Finance, U.S. Sec. and Exch. Comm'n).
14 Brian Quintenz, Comm'r, Commodity Futures Trading Comm'n, Keynote Address before the DC Blockchain Summit (Mar. 7, 2018), https://www.cftc.gov/PressRoom/SpeechesTestimony/opaquintenz8.
15 *Id.*
16 Brian Quintenz, Comm'r, Commodity Futures Trading Comm'n, Remarks Before the Eurofi High Level Seminar 2018 (Apr. 26, 2018).

If the CFTC determines that a digital token is a "commodity," then it may exercise general anti-fraud and anti-manipulation authority over "spot transactions" in that digital token. The CFTC defines spot transactions as those involving the exchange of a commodity for payment where immediate delivery and payment for the commodity is typically expected to occur on or within a few days of the transaction date.[17] In determining whether transfer of possession and control of the commodity has been made to the buyer, the CFTC considers: (i) "how the agreement, contract, or transaction is marketed, managed, and performed" and (ii) the facts regarding "[o]wnership, possession, title, and physical location," as well as the "relationship[s] between the buyer, seller, and possessor of the commodity… and the manner in which the… sale is recorded and completed."[18]

The CFTC's general anti-fraud and anti-manipulation rule ("Rule 180.1"), which was amended by the Dodd-Frank Wall Street Reform and Consumer Protection Act of 2010 to expand CFTC authority over spot transactions, prohibits persons "in connection with any… contract of sale of any commodity in interstate commerce" from:

- using or employing a manipulative device or scheme to defraud;
- engaging in or attempting to engage in market manipulation or fraud;
- making or attempting to make untrue or misleading statements of a material fact or omitting to state a material fact necessary in order to make statements made not untrue or misleading; and
- delivering false or misleading or inaccurate reports concerning market information or conditions that affect or tend to affect the price of a commodity.[19]

In a recent virtual currency-related regulatory action, the CFTC stated that Rule 180.1 grants it the "ability to bring enforcement actions for fraud or manipulation in connection with… contracts of sale of any commodity in interstate commerce."[20] Previously, the CFTC has relied upon Rule 180.1 to assert its jurisdiction over interstate trading in spot markets for commodities such as silver.[21] In September 2017, the CFTC cited Rule 180.1 in a complaint against a pooled fund operator for fraudulently inducing persons to invest in his bitcoin trading operation.[22] Commentators note that in this complaint, the CFTC "took a step beyond [its] traditional limit" of intervening in commodity spot markets only when "manipulative trading in the spot market affected the associated derivatives market."[23] At the time of the action, no Bitcoin futures market existed.

17 CFTC Letter No. 98-73, Comm. Fut. L. Rep. (CCH) P27,449 (Oct. 8, 1998), https://www.cftc.gov/sites/default/files/idc/groups/public/@lrlettergeneral/documents/letter/98-73.pdf.
18 Retail Commodity Transactions Under Commodity Exch. Act, 78 Fed. Reg. 52,426, 52428 (Aug. 23, 2013).
19 17 C.F.R. § 180.1(a) (2018).
20 Actual Delivery Proposed Interpretation, *supra* note 11 at fn 6.
21 *See* Complaint, CFTC v. Atlantic Bullion & Coin, Inc. and Ronnie Gene Wilson, S.C.D., No. 8:12-1503-JMC (June 6, 2012).
22 Complaint, CFTC v. Gelfman Blueprint, Inc. and Nicholas Gelfman, S.D.N.Y, No. 17-7181 (Sep. 21, 2017).
23 Brian T. Daly and Jacob Preiserowicz, *Bitcoin Derivatives and Expanded CFTC Jurisdiction*, Schulte Roth & Zabel (Nov. 14, 2017), https://www.srz.com/resources/bitcoin-derivatives-and-expanded-cftc-jurisdiction.html.

More recently, a March 2018 court ruling regarding a January 2018 CFTC complaint against market participants engaged in the non-leveraged purchase and sale of virtual currencies on behalf of retail customers found that the "CFTC may exercise its enforcement power over fraud related to virtual currencies sold in interstate commerce."[24] Notably, Litecoin, for which no futures market exists, was one of the virtual currencies traded on behalf of investors by the defendants in the complaint.

According to the CFTC, "a key component" of its "ability to effectively regulate [virtual currency] markets" is this ability to "assert legal authority over virtual currency derivatives in support of the CFTC's anti-fraud and manipulation efforts, including in underlying spot markets."[25] Thus the creation by the Chicago Mercantile Exchange ("CME") and Chicago Board Options Exchange ("CBOE") of futures markets for virtual currencies (limited to bitcoin futures to date) will likely lead to heightened CFTC scrutiny over the underlying spot markets for virtual currencies for which a corresponding, CFTC-regulated futures market exists.

Numerous retail customer-oriented spot markets have emerged through which market participants can convert virtual currency, fiat currency, or other digital tokens into other virtual currency, fiat currency, or other digital tokens. Entities that host these markets and that are neither (a) registered with the SEC pursuant to the Exchange Act as a "national securities exchange" or an "alternative trading system" nor (b) registered with the CFTC pursuant to the CEA as a "registered entity," are referred to in this report as "Token Trading Platforms." In some cases, as the CFTC recently noted, "[t]hese platforms provide a place to immediately exchange one commodity for another 'on the spot.'" There are a number of regulatory implications for these "centralized platforms" if a non-security digital token (being converted on a Token Trading Platform into another non-security digital token or into fiat currency) is deemed to be a virtual currency and thus a commodity by the CFTC. One important issue relates to "actual delivery" – a customer using a Token Trading Platform must, according to the CFTC's interpretation of CEA rules, receive "actual delivery" of that virtual currency within in 28 days of sale in order for the sales contract offered by the Token Trading Platform to be excluded from the definition of a futures contract, thus requiring it to be traded on a CFTC-regulated entity.

The CFTC has characterized virtual currencies as intangible commodities capable of actual delivery.[26] In an enforcement action involving Bitfinex, a Token Trading Platform, the CFTC found that actual delivery did not occur in that case because Bitfinex held customers' bitcoin in an omnibus settlement wallet in its own database rather than having transferred possession and control of the bitcoin to the customers.[27] The CFTC interpreted "actual delivery" to mean the delivery to a consumer of the

24 Memorandum & Order, CFTC v. Patrick K. McDonnell and Cabbagetech, Corp. d/b/a Coin Drop Markets, 3-4, (E.D.N.Y. 2018).
25 CFTC, CFTC Backgrounder on Oversight of and Approach to Virtual Currency Futures Markets (Jan. 4, 2018), http://www.cftc.gov/idc/groups/public/@newsroom/documents/file/backgrounder_virtualcurrency01.pdf.
26 *See* Actual Delivery Proposed Interpretation, *supra* note 11 at 60,337.
27 BFXNA INC. d/b/a Bitfinex, Order Instituting Proceedings Pursuant to Sections 6(c) and 6(d) of the CEA, as Amended, Making Findings and Imposing Remedial Sanctions, CFTC Docket No. 16-19 (June 2, 2016), https://www.cftc.gov/sites/default/files/idc/groups/public/@lrenforcementactions/documents/legalpleading/enfbfxnaorder060216.pdf.

purchased bitcoins' "private key" – the "secret number…associated with a deposit wallet that allows [the bitcoin] in that wallet to be spent."[28] That stance was challenged through a petition that noted:

"[M]aking control of private keys a prerequisite to having ownership and control of a cryptocurrency would be artificial and harmful to [cryptocurrency] markets because private keys have no innate legal significance with regard to the transfer, control, and possession of cryptocurrency on the blockchain… Rather, private keys are a modality to effectuate the parties' contractual agreements…and the significance or lack of significance of private keys…is determined entirely by the transacting parties."[29]

In December 2017, the CFTC issued a proposed interpretation regarding actual delivery of virtual currency, which notes that for actual delivery to occur, (1) a customer must have the ability to (i) "take possession and control" of the virtual currency, and (ii) "use it freely in commerce … no later than 28 days from the date of the transaction," and (2) the offeror or counterparty must not retain "any interest in or control over any of the [virtual currency]." Examples of actual delivery provided by the CFTC note that "title may be reflected by linking an individual purchaser with proof of ownership of the particular wallet to wallets that contain the purchased virtual currency."[30] A March 2018 court ruling calls the CFTC's stance into question, however, noting that "actual delivery" "does not require that a buyer take actual possession and control of the purchased commodities; it requires instead that the possession and control of commodities that exist in fact be transferred from the seller."[31]

Because the CFTC has deemed "virtual currency"[32] not to fall under the definition of "currency," it is not subject to a 2-day actual delivery requirement for retail foreign currency transactions. The agency, however, has requested public comment on whether a shortened actual delivery requirement would be appropriate for virtual currencies, and whether Congress should act to shorten the actual delivery requirement for these instruments.[33]

Regardless, in its Actual Delivery Proposed Interpretation, the CFTC noted that "depending on their use," tokens "may be commodities, commodity options, derivatives, or otherwise fall within the Commission's virtual currency definition described in this interpretation."[34] Indeed, agreements for the future delivery of digital tokens may qualify as derivatives contracts (futures or swaps) for an underlying commodity if the agreement includes optionality and/or does not provide for physical delivery. Such agreements can be thought of as commonplace commodity market forward agreements that provide for future delivery in instances where the commodity has not yet been

28 *Id.*
29 *See* Letter, ''Petition for Rulemaking Concerning the Requirements of 'Actual Delivery' and the Transfer of Ownership under the Commodity Exchange Act in the Context of Cryptocurrency Markets Utilizing Blockchain for Executing Transactions'' from Michael Dunn & Micah Green, Steptoe & Johnson LLP, to Chris Kirkpatrick, Secretary, CFTC (July 1, 2016), https://poloniex.com/press-releases/2016.10.18-Our-request- for-no-action-relief/Steptoe-Petition-for-CFTC- Rulemaking-(07-01-2016).pdf.
30 *Id.*
31 Tentative Order Regarding Motion to Dismiss, Motion for Preliminary Injunction, and Motion to Exclude, *CFTC v. Monex Deposit Co.*, et al., SACV 17-1868 JVS (DFM) (2018), (citing *CFTC v. Hunter Wise Commodities*, LLC, 749 F.3d 967, 970 (11th Cir. 2014)).
32 The CFTC has drawn a distinction between "real currency" – which it defined in the action as "the coin and paper money of the United States or another country that are designated as legal tender, circulate, and are customarily used and accepted as a medium of exchange in the country of issuance" – and "virtual currency." Coinflip Order *supra* note 9 at fn 2.
33 Actual Delivery Proposed Interpretation, *supra* note 11 at 60,335.
34 *Id.* at 60,341.

harvested or extracted for delivery. Such digital tokens would be subject to a variety of futures and swaps regulations as **"CFTC Regulated Instruments"** which, for purposes of this report, means any arrangement involving a digital token that would be subject to regulation by the CFTC as a future, swap, option or retail commodity transaction – as opposed to spot market transactions.

The likelihood that any arrangement involving a digital token may constitute a CFTC Regulated Instrument from the perspective of the CFTC is higher if the arrangement involves optionality, does not provide for immediate delivery of the token to the purchaser, the offer or sale of a commodity on a margined or financed basis where actual delivery does not occur within 28 days, or the exchange of one or more payments based on the value of one or more rates for, or prices of, intangible or tangible commodities.

B. TOKENIZED SECURITIES

The SEC and its staff have historically interpreted the definition of "security" under the Securities Act of 1933 (the "1933 Act" or the "Securities Act") and the Securities Exchange Act of 1934 (the "1934 Act" or the "Securities Exchange Act") broadly.[35] In addition to enumerating specific types of securities, such as stock and bonds, the 1933 Act definition of security also includes an "investment contract," which is essentially a catchall for securities that are not otherwise set out in Section 2(a)(1) of the 1933 Act. In the seminal 1946 case *SEC v. Howey*, noted above, interpreting the scope of the term "investment contract," the Supreme Court held that the term encompasses "a contract, transaction or scheme whereby a person invests his money in a common enterprise and is led to expect profits solely from the efforts of the promoter or a third party."[36] Under the *Howey* Test, an investment contract exists if there is: (1) an investment of money; (2) in a common enterprise; (3) with a reasonable expectation of profits; and (4) to be derived from the entrepreneurial or managerial efforts of others.[37]

In July 2017, the SEC considered whether so-called "initial coin offerings" involve, or could involve, the issuance of securities. It issued a Report of Investigation Pursuant to Section 21(a) of the Securities Exchange Act of 1934 in which it concluded, based on an investigation by its Division of Enforcement, that the digital tokens issued by the Decentralized Autonomous Organization (the "DAO") were securities (the "DAO Report") within the meaning of the 1933 Act and 1934 Act.[38] As described in the DAO Report, the DAO, an unincorporated association, issued tokens (the "DAO Tokens") via a website. Investors purchased DAO Tokens with ether. The DAO intended to use the funds it raised through the sale of DAO Tokens to fund "projects." DAO Token holders stood to share in the anticipated earnings from these projects as a return on their investment. After the initial issuance of the DAO Tokens, a secondary market for trading the DAO Tokens developed.

35 Robert H. Rosenblum, Chapter 2, Investment Company Determination under the 1940 Act: Exemptions and Exceptions, 2 (2003), https://apps.americanbar.org/buslaw/newsletter/0014/materials/investmentch2.pdf.
36 *W.J. Howey and Co.*, 328 U.S. at 298-299.
37 *Id.* at 301.
38 SEC, *Report of Investigation Pursuant to Section 21(a) of the Securities Exchange Act of 1934: The DAO*, Securities Act Release No. 81207 (July 25, 2017), https://www.sec.gov/litigation/investreport/34-81207.pdf.

In the DAO Report, the SEC analyzed whether the DAO Token was a security. Because a digital token such as the DAO Token is not a specifically-enumerated type of security under the 1933 Act, such as a stock or a bond, the SEC considered whether the DAO Token was an "investment contract."

To answer that question, the SEC applied the *Howey* Test and concluded that the DAO Tokens qualified as investment contracts and thus were securities for purposes of the Securities Act and the Exchange Act.[39] Specifically, the SEC found that:

- the purchase of DAO Tokens with ether was an "investment of money," noting that "money" need not take the form of cash;
- investors in DAO Tokens were investing in a common enterprise, *i.e.*, the DAO, which was created to pool resources and invest in a variety of projects;
- investors reasonably expected to earn profits by sharing in the return on projects that the DAO would fund from the proceeds of the DAO Token sales; and
- DAO Token holders' profits were to be derived from the managerial efforts of others, namely the founders and other key personnel associated with the DAO who would direct investments in projects.

Accordingly, the SEC concluded that DAO Tokens were securities that were issued without being registered under the Securities Act.

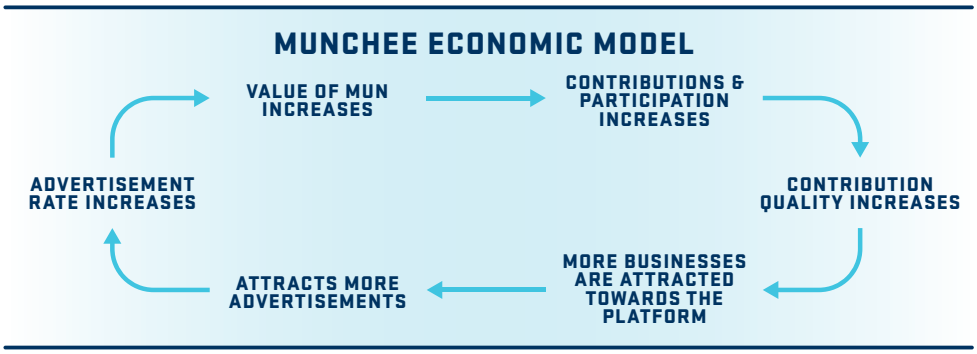
This was the first time that the SEC publicly found that a digital token constituted an investment contract under the Howey Test.

After publishing the DAO Report, the SEC brought a number of enforcement actions related to so-called ICOs. Most of those actions, however, were brought against persons who launched Ponzi schemes or other outright frauds.[40] Yet in the December 2017 *Munchee* Order, the SEC took the

39 *Id.*

40 Complaint, REcoin Group Foundation, LLC et al. (Sep. 29, 2017), http://www.sec.gov/litigation/complaints/2017/comp-pr2017-185.pdf; Complaint, SEC v. PlexCorps et al. (Dec. 1, 2017), http://www.sec.gov/litigation/complaints/2017/comp-pr2017-219.pdf; Order, Munchee, Inc. (Dec. 11, 2017), http://www.sec.gov/litigation/admin/2017/33-10445.pdf; Complaint, AriseBank et al. (Jan. 25, 2018), https://www.sec.gov/litigation/complaints/2018/comp-pr2018-8.pdf; Complaint, Jon E Montroll and Bitfunder (Feb. 21, 2018), https://www.sec.gov/litigation/complaints/2018/comp-pr2018-23.pdf; Complaint, Centra Tech., Inc. (Apr. 2, 2018), https://www.sec.gov/litigation/complaints/2018/comp-pr2018-70.pdf; Complaint, Longfin Corp., et al. (Apr. 6, 2018), http://www.sec.gov/litigation/complaints/2018/comp-pr2018-61.pdf.

opportunity to expand upon the DAO Report.[41] *Munchee* involved the creator of a restaurant review smartphone application, Munchee, that wanted to raise capital through the sale of digital tokens to expand its business. Munchee issued a white paper describing its proposed business expansion and plan to raise $15 million by issuing so-called "MUN tokens" in exchange for bitcoin and ether. Munchee characterized the MUN tokens as "utility tokens" and promised they could be used in the future to purchase goods and services in the ecosystem that Munchee would create. Munchee also stated that as use of its app increased, the value of MUN tokens would increase. Moreover, it promised to help increase the value of MUN tokens by "burning" tokens in the future, i.e., taking tokens out of circulation, and by working to ensure that the tokens would trade on a number of trading platforms.



The SEC's Division of Enforcement contacted Munchee and communicated its view that Munchee was engaged in an unregistered offering of securities in violation of the federal securities laws. Munchee terminated its offering, did not deliver any MUN tokens, and returned all proceeds it received from investors. In its cease-and-desist order concluding that MUN tokens were securities under the *Howey* Test, the SEC took the position that "[p]urchasers reasonably would have viewed the MUN token offering as an opportunity to profit… whether or not they ever used the Munchee App or otherwise participated in the MUN 'ecosystem.'"[42] Specifically, the SEC referenced online and social media statements made by Munchee in which, as the SEC notes, MUN token holders were told they "could count on the 'burning' of MUN tokens to raise the value of remaining MUN tokens." The order also highlights that Munchee promised to take action to increase the value of MUN tokens by expanding its business and agreed to use its efforts to allow investors to take advantage of the increased value of MUN tokens by helping to establish a secondary market that would allow holders to sell their tokens. That profit, moreover, would derive from the entrepreneurial efforts of Munchee and its agents, who were working to build out Munchee. The SEC also emphasized that characterizing a digital token as a "utility token" was not in and of itself sufficient to take MUN tokens outside of the definition of a security, even if the tokens had practical use. Rather, the key was the economic reality underlying a

41 Munchee Inc., Securities Act Release No. 10445 (Dec. 11, 2017), https://www.sec.gov/litigation/admin/2017/33-10445.pdf.
42 *Id.*

token sale; yet the *Munchee* Order made clear that MUN tokens had no utility at the time of issuance outside of their potential to trade on the secondary market, given that Munchee had not yet built out its ecosystem.

Since *Munchee*, the SEC has continued to urge caution with respect to digital token distributions. Chairman Clayton remarked during a February 2018 United States Senate hearing that he views many new digital tokens to be securities,[43] although more recently, he noted that it is "absolutely not" the case that all digital tokens are securities.[44] Yet, as Chairman Clayton explained during his February testimony, and as noted in the DAO Report, whether a digital token distribution involves a security is a facts-and-circumstances determination.

Of course, as explained above, SEC officials appear to recognize that some digital tokens are not securities.[45] Notably, the SEC did not deem ether to be a security in its DAO Report, and both the SEC and Chairman Clayton seemingly draw a distinction between "coins" (such as virtual currencies, which are commodities) and "virtual tokens."[46] With regard to the distinction between securitized tokens and other digital tokens, Chairman Clayton remarked in 2017,

"A KEY QUESTION FOR ALL ICO MARKET PARTICIPANTS IS, 'IS THE COIN A TOKEN OR A SECURITY?'"

- Chairman Jay Clayton, U.S. Securities and Exchange Commission

"A key question for all ICO market participants: 'Is the coin or token a security?' As securities law practitioners know well, the answer depends on the facts. For example, a token that represents a participation interest in a book-of-the-month club may not implicate our securities laws and may well be an efficient way for the club's operators to fund the future acquisition of books and facilitate the distribution of those books to token holders."[47]

43 *Virtual Currencies: The Oversight Role of the U.S. Securities and Exchange Commission and the U.S. Commodity Futures Trading Commission: Hearing Before the S. Comm. on Banking, Housing, and Urban Affairs*, 115th Cong. (2018) (statement of Jay Clayton, Chairman, U.S. Sec. and Exch. Comm'n).

44 Nikhilesh De and Mahishan Gnanaseharan, *SEC Chief Touts Benefits of Crypto Regulation*, COINDESK (Apr. 5, 2018), https://www.coindesk.com/sec-chief-not-icos-bad/.

45 *See supra* notes 13 to 15 and accompanying text.

46 SEC, *Statement Urging Caution Around Celebrity Backed ICOs*, (Nov. 1, 2017), https://www.sec.gov/news/public-statement/statement-potentially-unlawful-promotion-icos; SEC, *Investor Bulletin: Initial Coin Offerings,* (July 25, 2017), https://www.investor.gov/additional-resources/news-alerts/alerts-bulletins/investor-bulletin-initial-coin-offerings.

47 SEC, *Statement on Cryptocurrencies and Initial Coin Offerings*, (Dec. 11, 2017), https://www.sec.gov/news/public-statement/statement-clayton-2017-12-11.

Furthermore, in April 2018, he stated that digital tokens can evolve from being securities into non-securities, using the example of a laundry token:

"If I have a laundry token for washing my clothes, that's not a security. But if I have a set of 10 laundry tokens and the laundromats are to be developed and those are offered to me as something I can use for the future and I'm buying them because I can sell them to next year's incoming class, that's a security. . .What we find in the regulatory world [is that] the use of a laundry token evolves over time. . .[and] [t]he use can evolve toward or away from a security."[48]

No formal SEC statement exists listing the criteria under which the SEC would determine that a particular digital token is or is not a security. As explained above, the SEC relies upon facts and circumstances using the *Howey* Test and has provided insights into its digital token-specific considerations in these matters through the DAO Report and the *Munchee* enforcement action. If the SEC does determine that a particular digital token is a security, then a panoply of federal securities laws applies to the distribution and trading of that token, as outlined below.

1. REGISTRATION OF OFFERS AND SALES

Section 5 of the Securities Act prohibits the sale of securities to the public unless a registration statement for such securities has been filed with the SEC and is in effect, and the issuer has delivered a prospectus to investors. The SEC's DAO Report observes that the term "issuer" is flexibly construed, and, therefore, that The DAO was an issuer required to provide needed information material to the investors in deciding whether to purchase the DAO Tokens.

Section 12(a)(1) of the Securities Act imposes liability on persons who offer or sell securities in violation of Section 5.[49] Under limited circumstances, offers to sell securities can be made prior to the filing of a registration statement (pre-filing period). There is no defined period as to when the pre-filing period commences; therefore, token issuers should consider whether publishing of white papers on websites could be construed as an offer to sell.

There are several potential exemptions from the registration requirements, including:

» Section 4 of the Securities Act permits sales of securities without registration with the SEC under specified circumstances:

- Section 4(a)(2) Non-public offerings – Issuers must limit sales to so-called "sophisticated investors" who have sufficient knowledge and experience in finance and business to evaluate the risks and merits of investment, or who have the ability to bear the risk of loss associated with the investment.

48 De and Gnanaseharan, *supra* note 46.
49 Violations of securities laws are subject to civil and criminal penalties.

- Section 4(a)(5) – This paragraph permits non-public offers and sales made solely to accredited investors (a term discussed below), up to a maximum issuance of $5 million.
- Section 4(a)(6) – This paragraph provides a crowdfunding exemption that permits the issuance of securities that does not exceed $1 million in value. It also imposes maximum amounts that individual investors may invest in a given crowdfunding offering.
- Section 4(a)(7) – This paragraph provides that sales of securities are permitted where, among other things, issuers have limited sales to accredited investors; have not engaged in general solicitation or general advertising, and make specified information available to prospective purchasers, including the issuer's most recent balance sheet and profits and loss statement, as well as similar financial statements.

» Rules 504 and 506 of Regulation D under the Securities Act[50] – Regulation D is intended to clarify the scope and requirements of certain securities offering exemptions under Section 4 of the Securities Act. The rules permit issuance of securities without SEC registration. Securities offerings under Rule 504 are open both to accredited and non-accredited investors,[51] but general solicitation of investors is prohibited. Offerings under Rule 506 are limited to accredited investors, but general solicitation is permitted for offerings conducted under paragraph (c) of Rule 506 (intended to allow access to the capital markets for small companies unable to bear costs of normal registration. Sales are generally limited to accredited investors.)

» Regulation A under the Securities Act – allows companies to raise money under two different tiers:

- Tier 1 – eligible up to $20 million in a 12-month period; requires an offering circular to be filed with and qualified by the SEC as well as relevant state regulators; submission of unaudited financial statements; no ongoing reporting obligations.
- Tier 2 – eligible up to $50 million in a 12-month period; requires an offering circular to be filed with and qualified by the SEC; submission of audited financial statements; and ongoing reporting obligations.

Issuers also need to be aware of potential state law securities registration requirements.

50 17 C.F.R. § 230.500 *et seq.* (2018).

51 Under Rule 501 of Regulation D, the term "accredited investor" includes, among others, certain financial institutions, such as broker-dealers, registered investment companies and insurance companies. It also includes natural persons whose net worth, or joint net worth with that person's spouse, exceeds $1 million (excluding the value of the person's residence). The term also includes natural persons whose income in each of the two most recent years was in excess of $200,000 or jointly with that person's spouse was in excess of $300,000.

2. SECONDARY MARKET TRADING

Investors can resell securities that they acquire in private and public offerings in private transactions, on registered securities exchanges or in over-the-counter ("OTC") transactions. Each type of resale transaction is subject to certain requirements and considerations. This report focuses on secondary market transactions on exchanges and OTC markets.

Both the exchanges and the securities that trade on them are subject to requirements under the Exchange Act. Section 5 of the Exchange Act makes it unlawful to effect any transaction in a security on an exchange unless it is registered as a national securities exchange under Section 6 of the Exchange Act or exempted from such registration. An exchange is defined as "a marketplace or facilities for bringing together purchasers and sellers of securities."[52] In the DAO Report, the SEC concluded that the platforms that permitted secondary market trading in DAO Tokens were unregistered exchanges not exempt from registration and, thus, their trading of DAO Tokens, which were securities, violated Section 5 of the Exchange Act.

Securities that trade on an exchange are either listed to trade on that exchange, or entitled to unlisted trading privileges on that exchange (a security may obtain unlisted trading privileges on an exchange only if it is listed on another exchange). Section 12 of the Exchange Act prohibits a security from trading on a national securities exchange unless there is in place an effective registration with respect to that security for the exchange. Exchanges display quotations in securities in accordance with applicable securities laws, regulations and rules, such as Regulation NMS.[53]

Securities can also trade on an OTC basis, typically on alternative trading systems ("ATS"). An ATS is a marketplace that provides for secondary market trading of securities. Instead of registering as a national securities exchange, however, an ATS registers as a broker-dealer and files Form ATS with the SEC in accordance with the requirements of Regulation ATS.[54] An ATS does not list securities. Rather, an ATS typically displays quotations in securities that broker-dealer subscribers to the ATS provide in compliance with Rule 15c2-11 under the Exchange Act. Rule 15c2-11 requires a broker-dealer wishing to publish any quotation for a security in a "quotation medium" (which includes an ATS) to gather specified information regarding the issuer.[55] Securities issued in a private placement, however, are not freely tradeable and, thus, cannot be subject to quoting on an ATS unless and until they have met certain requirements, such as a six-month or one-year restricted period, i.e., a period during which the security may not be traded, as set out in Rule 144 under the Securities Act.[56]

52 Exchange Act Section 3(a)(1), 15 U.S.C. § 78c(a)(1) (2012), and Exchange Act Rule 3b-16(a), 17 C.F.R. § 240.3b-16(a) (2018).
53 17 C.F.R. § 242.600 *et seq.* (2018).
54 17 C.F.R. § 242.300 *et seq.* (2018).
55 17 C.F.R. § 240.15c2-11 (2018).
56 17 C.F.R. § 230.144 (2018).

3. ANTI-FRAUD, ANTI-MANIPULATION, AND RELATED RULES

Federal securities laws, rules, and regulations (*e.g.*, Rule 10b-5 under the Exchange Act) prohibit, directly or indirectly, fraud and manipulation in connection with the purchase or sale of any security as well as with security-based swap transactions. Such behavior includes: (a) fraudulent or deceitful devices and schemes; and (b) material misstatements or omissions.

Separately, Section 11(a) of the Securities Act imposes liability for untrue statements of material facts in registration statements, or omissions of material facts that are needed to make statements in registration statements not misleading. Furthermore, Section 12(a)(2) of the Securities Act allows for the rescission of securities purchases (or a suit for damages) if the offer/sale was made using a prospectus or oral communication containing material misstatements or omissions.

Additionally, there are a number of state laws, such as the Martin Act of New York State, related to fraud and manipulation in securities markets.

4. OTHER ISSUES

If a derivatives market emerges for which the underlying asset is a tokenized security, either the SEC or the CFTC would regulate the derivatives. Options, swaps on single names or narrow indexes, or futures on single names would be subject to the SEC's jurisdiction. Swaps on broad-based indices and futures on other than single names would be subject to CFTC jurisdiction.

A person that "engages on behalf of an issuer of securities or on behalf of itself in… transferring record ownership of securities by bookkeeping entry without physical issuance of securities certificates" would fall within the definition of "transfer agent" in the Exchange Act.[57] Unless exempted, a transfer agent that makes use of the jurisdictional means to perform that function with respect to a security registered under Exchange Act Section 12[58] must register as such with the SEC.[59] Therefore, a system that uses distributed ledger technology to electronically transfer record ownership of securities as or on behalf of an issuer may be subject to the registration requirements of Section 17A of the Exchange Act.

C. WHEN DIGITAL TOKENS ARE NEITHER SECURITIES NOR COMMODITIES

As suggested earlier, it is possible – and perhaps appropriate – for some digital tokens to be viewed as neither a security nor a commodity by regulators. In these instances, digital tokens can bear a closer resemblance to participatory rights in channels of communication, collaboration, and commerce, rather than as an intangible commodity or security that is bought and sold.

57 15 U.S.C. § 78c(a)(25)(E) (2012). Other provisions of the definition also may be relevant to this discussion. *See, e.g.*, § 78c(a)(25)(B) and (C) (2012).
58 15 U.S.C. § 78l (2012).
59 78 U.S.C. § 78q-1(c)(1) (2012).

For example, airline miles and other loyalty and rewards points programs constitute neither securities nor commodities. Yet points in many such programs can oftentimes be purchased for fiat currency and even transferred for cash. Of course, these instruments are not generated using blockchain technology, but nonetheless illustrate that in the United States regulatory context it is plausible that cash conversion markets for particular tokens could exist, even though tokens do not constitute securities or commodities, but rather, participatory rights in a system of communication or commerce.

Federal and state consumer protection laws and escheat laws apply to gift cards, gift certificates, and similar kinds of property, and presumably would apply to tokens that are neither securities nor commodities. Indeed, the broader regulatory considerations set forth below apply not just to tokens that are neither securities nor commodities, but also to all other digital tokens, broadly defined.

III. BROADER REGULATORY CONSIDERATIONS

A. CONSUMER PROTECTION ISSUES

Regardless of the legal category (security versus commodity versus neither) of a particular digital token, state attorneys general ("AG") would have jurisdiction to enforce their states' consumer protection and anti-fraud statutes as those laws relate to the purchase and sale of tokens. AG offices would likely have jurisdiction to bring enforcement actions if residents of their states were affected, or if bad actors conducted business in their state. The FTC is also charged with protecting consumers from unfair or deceptive acts and practices that affect commerce.[60] The FTC has authority to conduct investigations, issue subpoenas, and file enforcement actions in administrative tribunals or in federal court. If securities laws do not apply, it is likely that the FTC would have jurisdiction to bring antifraud claims against bad actors.[61] In 2014, the Consumer Financial Protection Bureau ("CFPB") issued a statement regarding virtual currency products and services, noting that it will use complaints it receives from consumers regarding bitcoin and other virtual currencies to "help enforce federal consumer financial laws and, if appropriate, take consumer protection policy steps."[62] So far, the agency has yet to take any enforcement actions related to virtual currencies or digital tokens. Notably, in 2016, the Bureau's final prepaid card rule was issued without referring to virtual currency products within its "prepaid access" definition, and the agency stated that the "application of Regulation E and this final rule to [virtual currency] products and services" was "outside of the scope" of its rulemaking.[63] It also noted that, "as part of its broader administration and enforcement of the enumerated consumer financial protection statutes and Title X of the Dodd-Frank Act, the Bureau continues to analyze the nature of products or services tied to virtual currencies."[64]

60 *See* Federal Trade Commission Act, 15 U.S.C. § 45(a)(1) (2012).
61 *See, for example*, Complaint for Permanent Injunction and Other Equitable Relief at 1-2, FTC v. BF Labs, Inc., No. 4:14-cv-0815 (W.D. Mo. Sept. 15, 2014). For more information on this case, see Darren J. Sandler, "Citrus Groves in the Cloud: Is Cryptocurrency Cloud Mining a Security?," 34 SANTA CLARA HIGH TECHNOLOGY LAW JOURNAL 250, 267-268 (Jan. 2018).
62 CFPB, *CFPB Warns Consumers About Bitcoin*, (Aug. 11, 2014), https://www.consumerfinance.gov/about-us/newsroom/cfpb-warns-consumers-about-bitcoin/.
63 CFPB, *Prepaid Accounts under the Electronic Fund Transfer Act (Regulation E) and the Truth In Lending Act (Regulation Z)*, 164 (Oct. 3, 2016), https://files.consumerfinance.gov/f/documents/20161005_cfpb_Final_Rule_Prepaid_Accounts.pdf.
64 *Id*.

B. STATE MONEY TRANSMISSION LAWS

Trading Platforms that receive for transmission or transmit U.S. dollars in exchange for virtual currency are regulated as money transmitters in many U.S. states in which they operate or have customers. Money transmitter regulatory regimes entail a variety of regulations aimed primarily at protecting consumers, which often include regular examinations, minimum net worth standards, disclosures of key employee criminal convictions, descriptions of the organization's structure, and a copy of recent audited financial statements.[65] Some state regulatory regimes may entail particularly stringent obligations and/or may be geared particularly towards firms engaged in the purchase, sale, generation, or distribution of convertible virtual currencies. For example, the New York Department of Financial Services "BitLicense" requirements are triggered when a company engages in a "virtual currency business activity." All holders of a BitLicense must maintain a written anti-fraud policy as well as other enumerated policies. Further, federal law makes it a crime to fail to obtain state money transmitter licenses when required to do so.[66]

C. ANTI-MONEY LAUNDERING AND SANCTIONS REGULATIONS

Anti-money laundering ("AML") regulations and associated requirements are significantly important to how digital tokens can be distributed and purchased. The relevant AML rules relate to the Bank Secrecy Act ("BSA"),[67] which requires financial institutions to comply with recordkeeping and reporting requirements, and to develop and implement AML compliance regimes. Similar requirements exist for asset management firms and broker-dealers, including under FINRA Rule 3310. Money transmitters must also register as money services businesses ("MSBs") with the United States Treasury Department's Financial Crimes Enforcement Network ("FinCEN").

The sanctions programs maintained by the Office of Foreign Assets Control ("OFAC") also apply to digital token market participants.

Companies engaged in financial transactions are advised to maintain both AML and OFAC compliance programs to ensure they do not run afoul of these obligations and restrictions. To maintain compliance with both of these regimes, companies must have some understanding of persons with whom they interact.

1. BANK SECRECY ACT & RELATED REGULATORY REQUIREMENTS

In 1970, the United States Congress passed the Currency and Foreign Transactions Reporting Act, commonly known as the BSA, which established requirements for recordkeeping and reporting by private individuals, banks, and other financial institutions. The BSA was designed to help identify the source, volume, movement of currency and other monetary instruments

65 CSBS, *The State of State Money Service Businesses Regulation and Supervision*, (May 2016), https://www.csbs.org/sites/default/files/2017-11/State%20of%20State%20MSB%20Regulation%20and%20Supervision%202.pdf.
66 18 U.S.C. § 1960 (2012).
67 31 U.S.C. § 5311 *et seq* (2012); 12 U.S.C. §§ 1829b, 1951-1959 (2012).

transported or transmitted into or out of the United States or deposited in financial institutions. The statute requires individuals, banks, and other financial institutions to file reports with the United States Department of the Treasury, properly identify persons conducting transactions, and maintain appropriate records of financial transactions. These reports and records enable law enforcement and regulatory agencies to pursue investigations of criminal, tax, and regulatory violations, and provide evidence useful in prosecuting money laundering and other financial crimes.

Various statutes since then expanded on the authority of the BSA, including the Money Laundering Control Act of 1986, the Annunzio-Wylie Anti-Money Laundering Act of 1992, the Money Laundering Suppression Act of 1994, and the Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001 ("USA PATRIOT Act").

Pursuant to guidance published on March 18, 2013 by the FinCEN, the Treasury agency charged with administering and enforcing the BSA, "administrators" and "exchangers" of convertible virtual currency are treated as money transmitters under the BSA and are thus subject to its AML requirements. [68]

Specifically, money transmitters – such as certain Trading Platforms – must develop, implement, and maintain effective AML programs that address the ever-changing strategies of money launderers and terrorists who attempt to gain access to the United States financial system.

ANTI-MONEY LAUNDERING COMPLIANCE PROGRAM MINIMUM ELEMENTS

1

A SYSTEM OF POLICIES, PROCEDURES, AND INTERNAL CONTROLS

2

A DESIGNATED BSA OFFICER

3

TRAINING FOR APPROPRIATE PERSONNEL

4

INDEPENDENT TESTING

68 FIN-2013-G001, *Application of FinCEN's Regulations to Persons Administering, Exchanging, or Using Virtual Currencies* (Mar. 18, 2013). Note that money transmitters must also obtain state money transmitter licenses in almost every U.S. state and territory. Failure to do so constitutes a federal crime under 18 U.S.C. § 1960.

At a minimum, an AML compliance program must contain the following elements:

1. A system of policies, procedures, and internal controls to ensure compliance with the BSA;
2. A designated BSA Officer who is responsible for ensuring the Company's compliance with the BSA and Office of Foreign Assets Control ("OFAC") requirements;
3. Training for appropriate personnel; and
4. Independent testing of the program.

The program must also address specific recordkeeping and reporting obligations, such as filing suspicious activity reports ("SARs") and currency transaction reports ("CTRs").

Similar requirements apply to broker-dealers,[69] mutual funds,[70] and futures commission merchants and introducing commodity brokers.[71] Broker-dealers also must comply with FINRA's AML compliance rule, FINRA Rule 3310.[72] Further, general prohibitions against promoting or conducting a transaction knowing the proceeds facilitate money laundering or other crimes, whether or not a company is a "financial institution" under the BSA, apply to all persons.[73]

Appropriate procedures for KYC at customer onboarding and then monitoring the customer's ongoing transactions are essential to determining whether suspicious activity is occurring.

It is also worth noting that various state regulatory regimes may entail additional AML standards. For example, holders of New York's "BitLicense" must, among other things:

- Conduct AML risk assessments, and maintain and enforce an AML program very similar in structure to that required by FINRA Rule 3310;
- Verify customer identities at account opening and maintain transaction records that reflect the identity and physical addresses of customers and other parties to the transaction to the extent practicable;
- File SARs as required under federal law, and make certain SAR-like filings to NY state if not required to make such filings to federal regulators; and
- Maintain a written anti-fraud policy.

2. OFFICE OF FOREIGN ASSETS CONTROL REQUIREMENTS

The Office of Foreign Assets Control ("OFAC") administers and enforces both comprehensive and targeted economic and trade sanctions to further United States foreign policy and

69 31 C.F.R. § Part 1023 (2018).
70 31 C.F.R. § Part 1024 (2018).
71 31 C.F.R. § Part 1026 (2018).
72 FINRA Rule 3310.
73 18 U.S.C. §§ 1956, 1957 (2012).

national security goals against certain foreign countries and regimes, nationals of certain of those countries, designated terrorists, foreign terrorist organizations, international narcotics traffickers, those engaged in activities related to the proliferation of weapons of mass destruction, and other threats to the national security, foreign policy, or the economy of the United States. OFAC acts under Presidential national emergency powers, as well as authority granted by specific legislation, to impose controls on transactions and freeze assets under United States jurisdiction.

OFAC requirements apply to all "U.S. persons" or "Persons subject to U.S. jurisdiction", including United States incorporated companies and their foreign branches, persons and companies located or physically in the United States, and United States citizens and permanent resident aliens wherever located. In certain sanctions programs, foreign subsidiaries owned or controlled by United States companies must also comply.

The specific prohibitions vary depending on the program; however, OFAC sanctions generally prohibit transactions or dealings with a person or entity identified on the OFAC list of Specially Designated Nationals and Blocked Persons (the "SDN List") or the assets of a SDN, as well as certain transactions and activities with countries or sectors subject to economic sanctions. OFAC regulations maintain specific instructions on what to do if such a transaction or dealing is attempted, including "blocking" (freezing) of accounts or property, or prohibiting or rejecting the transaction.

3. EXECUTIVE ORDER 13827 AND VENEZUELA-RELATED SANCTIONS

On January 19, 2018, OFAC published FAQ 551 stating that United States persons who engage in purchasing or otherwise dealing with the Venezuelan petro (a state-sponsored virtual currency backed by oil) may violate United States sanctions imposed against Venezuela because of rights attached to it to receive commodities, such as oil, in a specified quantity at a later date.[74] This right to receive commodities would violate Executive Order 13808, issued on August, 24, 2017, which, among other things, prohibits transactions, financing, and other dealings regarding "new debt with a maturity of greater than 30 days, or new equity, of the Government of Venezuela."[75]

On March 19, 2018, President Trump signed Executive Order 13827, Taking Additional Steps to Address the Situation in Venezuela and memorializing the policy position taken in FAQ 551. This Executive Order provides that United States persons may not transact, deal, or provide financing related to any digital currency, digital coin, or digital token that was issued by, or on behalf of the Government of Venezuela on or after January 9, 2018.[76] Executive Order 13827 also

74 OFFICE OF FOREIGN ASSETS CONTROL, FAQ 551 (2018). Superseded by Exec. Order No. 13,827 (Mar. 19, 2018), 83 Fed. Reg. 12,469 (2018), https://www.federalregister.gov/d/2018-05916.
75 *Id.*
76 Exec. Order No. 13,827 (Mar. 19, 2018), 83 Fed, Reg. 12,469 (2018), https://www.federalregister.gov/d/2018-05916.

covers the broad concepts of "digital currency," "digital coin," and "digital token," which are undefined in the Order but are explained in OFAC FAQs 564-566.

Following the issuance of Executive Order 13827, OFAC amended its list of FAQs related to sanctions imposed against Venezuela to add FAQs 564-66. FAQ 564 clarifies that for the purposes of Executive Order 13827, Venezuela's petro and petro-gold are considered to be a digital currency, digital coin, or digital token issued by the Government of Venezuela on or after January 9, 2018; thereby prohibiting transactions by United States persons related to the petro and petro-gold.[77] FAQ 565 clarifies that Venezuela's fiat currency, the bolivar fuerte, does not constitute a digital currency, digital coin, or digital token. Finally, FAQ 566 provides that OFAC would consider license applications related to digital currencies, digital coins, or digital tokens issued by the Government of Venezuela on a case-by-case basis, but generally, absent OFAC's authorization, United States persons may not "engag[e] in transactions related to, provid[e] financing for, and otherwise deal" in Venezuelan-issued digital currencies, digital coins, or digital tokens.

On March 19, 2018, OFAC amended its FAQs to clarify its policy position on virtual currencies generally.[78] FAQ 559 defines "virtual currency," "digital currency," "digital currency wallet," and "digital currency address."[79]

FAQ 560 states that OFAC compliance obligations are the same for United States persons whether transactions are denominated in a digital currency or a traditional fiat currency. Further, OFAC specifically notes that the compliance obligations extend to firms that are using

77 OFFICE OF FOREIGN ASSETS CONTROL, FAQ 564-66 (2018), https://www.treasury.gov/resource-center/faqs/Sanctions/Pages/faq_other.aspx#venezuela.

78 OFFICE OF FOREIGN ASSETS CONTROL, FAQ 559 (2018), https://www.treasury.gov/resource-center/faqs/Sanctions/Pages/faq_compliance.aspx.

79 *Id.* Virtual currency is defined as a "digital representation of value that functions as (i) a medium of exchange; (ii) a unit of account; and/or (iii) a store of value; is neither issued nor guaranteed by any jurisdiction; and does not have legal tender status in any jurisdiction." Digital currency "includes sovereign cryptocurrency, virtual currency (non-fiat), and a digital representation of fiat currency." *Id.* Digital currency wallet is defined as "a software application (or other mechanism) that provides a means for holding, storing, and transferring digital currency. A wallet holds the user's digital currency addresses, which allow the user to receive digital currency, and private keys, which allow the user to transfer digital currency. The wallet also maintains the user's digital currency balance. A wallet provider is a person (individual or entity) that provides the software to create and manage wallets, which users can download. A hosted wallet provider is a business that creates and stores a digital currency wallet on behalf of a customer. Most hosted wallets also offer exchange and payments services to facilitate participation in a digital currency system by users." *Id.* Digital currency address is defined as "an alphanumeric identifier that represents a potential destination for a digital currency transfer. A digital currency address is associated with a digital currency wallet." *Id.*

digital currency when facilitating or engaging in online commerce or processing transactions, as well as trading platforms and others. In addition, the FAQ states that technology companies, digital currency users, digital currency trading platforms, digital currency administrators, and other payment processors, among others, should develop tailored, risk-based compliance programs that include sanctions list screening.

FAQ 561 explains that OFAC will use pre-existing government strategies designed to combat illicit use of digital currencies in order to sanction perpetrators. In addition, OFAC reserved the right to amend its SDN list to include specific digital currency addresses that are associated with blocked persons or entities that appear on the list.

FAQ 562 explains that OFAC may also add digital currency addresses associated with blocked persons to the SDN list, and reminds companies that any such digital currency must be blocked and to file a blocking report with OFAC.

FAQ 563 states that the format in which a digital currency address is included on the SDN list will include its corresponding digital currency.

D. FEDERAL INCOME TAX TREATMENT

The federal income tax consequences of transactions involving digital tokens is a developing area of law. The IRS has issued some guidance in Notice 2014-21, which generally treats convertible virtual currencies as property for United States tax purposes, rather than, for example, as foreign currency. However, Notice 2014-21 does not cover all of the terrain, and there are a number of areas of remaining uncertainty.

1. TREATMENT OF CONVERTIBLE VIRTUAL CURRENCIES UNDER NOTICE 2014-21

In April 2014, the IRS issued Notice 2014-21, which explains, in question and answer format, the application of existing general tax principles to transactions using virtual currency.

The guidance in the Notice only applies to "convertible virtual currency," defined as "[v]irtual currency that has an equivalent value in real currency, or that acts as a substitute for real currency." The Notice cited bitcoin as one example of a convertible virtual currency, noting that it "can be digitally traded between users and can be purchased for, or exchanged into, United States dollars, Euros, and other real or virtual currencies."

The Notice provides that, in general, the sale or exchange of convertible virtual currency, or the use of convertible virtual currency to pay for goods or services in a real-world economy transaction, has tax consequences that may result in a tax liability. The Notice provides that virtual currency is treated as property for tax purposes and that "[g]eneral tax principles applicable to property transactions" apply to transactions using virtual currency.

The Notice provides that virtual currency is not treated as currency that could generate foreign currency gain or loss for tax purposes.

The Notice describes some of the tax consequences of mining virtual currency. The Notice provides that when a taxpayer successfully mines virtual currency, the fair market value of the virtual currency as of the date of receipt is includible in gross income. The Notice further provides that if a taxpayer's mining of virtual currency constitutes a trade or business, and the mining activity is not undertaken by the taxpayer as an employee, the net earnings resulting from those activities constitute self-employment income and are subject to the self-employment tax.

The Notice also describes some of the tax consequences of exchanging virtual currency for other property. If the fair market value of property received in exchange for virtual currency exceeds the taxpayer's adjusted basis of the virtual currency, the taxpayer has taxable gain. The taxpayer has a loss if the fair market value of the property received is less than the adjusted basis of the virtual currency. The Notice provides that the basis of virtual currency is generally equal to the fair market value of the virtual currency in United States dollars as of the date of receipt. The Notice also provides that if a virtual currency is listed on an exchange and the exchange rate is established by market supply and demand, the fair market value of the virtual currency is determined by converting the virtual currency into United States dollars (or into another real currency which in turn can be converted into United States dollars) at the exchange rate, in a reasonable manner that is consistently applied.

The character of the gain or loss generally depends on whether the virtual currency is a capital asset in the hands of the taxpayer. Virtual currency held for investment typically should be treated as a capital asset. Virtual currency held mainly for sale to customers in a trade or business typically should not be treated as a capital asset. In general, gain on the sale or exchange of a capital asset is treated as long-term capital gain (taxed at preferential rates) when the capital asset has been held for longer than one year. When a capital asset has been held for less than one year, gain generally is treated as short-term capital gain (taxed at ordinary income rates). Gain on the sale or exchange of a non-capital asset generally is treated as ordinary income.

The Notice provides that payments made using virtual currency are subject to information reporting to the same extent as any other payment made in property. The fair market value of virtual currency paid as wages is subject to federal income tax withholding, Federal Insurance Contributions Act ("FICA") tax, and Federal Unemployment Tax Act ("FUTA") tax and must be reported on Form W-2. Generally, a person who in the course of a trade or business makes a payment of $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. A third party that contracts with a substantial number of unrelated merchants to settle payments between the merchants and their customers is a third-party settlement organization that is required to report payments made to a merchant on a Form 1099-K.

Payments made using virtual currency are subject to backup withholding to the same extent as other payments made in property. Therefore, payors making reportable payments using virtual currency must solicit a taxpayer identification number ("TIN") from the payee. The payor must backup withholding from the payment if a TIN is not obtained prior to payment or if the payor receives notification from the IRS that backup withholding is required.

2. OTHER TAX ISSUES INVOLVING VIRTUAL CURRENCIES

Notice 2014-21 does not provide guidance on certain issues relating to the tax treatment of virtual currencies, including: (i) whether and how virtual currency brokers or dealers must report transactions involving virtual currency on Form 1099-B; (ii) whether holders of virtual currency should report their holdings on FinCEN Form 114 (FBAR reporting) or Form 8938 (FATCA reporting); (iii) the circumstances under which two different kinds of virtual currency may be regarded as like kind property for purposes of Section 1031 of the Internal Revenue Code; and (iv) the treatment of a "hard fork" in the blockchain of a virtual currency or of an "airdrop" of virtual currency.

In general, a broker or dealer that effects the sale of certain securities, commodities, options, regulated futures contracts, securities futures contracts, or forward contracts by a customer in the ordinary course of a trade or business must report information concerning its customer's name, address, and TIN, the property sold, the gross proceeds of the sale, the sale date, and other information required by Form 1099-B. In addition, with respect to certain "covered securities," the broker or dealer must report the adjusted basis of the security sold and whether any gain or loss with respect to the security sold is long-term or short-term. If reportable sales are not reported on a Form 1099-B, then the broker or dealer generally is subject to backup withholding. Treasury and the IRS have not produced guidance on whether or how brokers or dealers should comply with Form 1099-B reporting with respect to virtual currency.

In general, United States persons that have a financial interest in or signature authority over foreign financial accounts that exceed specified value thresholds must file a Report of Foreign Bank and Financial Accounts ("FBAR"), Form 114, through the e-filing system of FinCEN. In addition, under the Foreign Account Tax Compliance Act ("FATCA"), certain taxpayers that have an interest in specified foreign financial assets that exceed specified value thresholds must report those assets on a Statement of Specified Foreign Financial Assets, Form 8938, filed with their annual tax return. Treasury, the IRS, and FinCEN have not produced any guidance on whether virtual currency accounts could be subject to these reporting requirements.

Prior to 2018, under Section 1031 gain or loss generally was not recognized on the sale or exchange of property held for productive use in a trade or business or for investment if such property was exchanged solely for property of like kind which was to be held either for productive use in a trade or business or for investment. Whether intangible personal property

was of a like kind to other intangible personal property generally depended on the nature and character of the rights involved and on the nature or character of any underlying property. Treasury and the IRS have not issued guidance on the circumstances under which two different kinds of virtual currency may be regarded as like kind property for purposes of Section 1031. The IRS has historically taken a narrow view of the type of property that can qualify as like-kind (for example, treating gold and silver bullion or gold numismatic and gold bullion coins as not like-kind but treating gold bullion for Canadian Maple Leaf gold coins or Mexican and Austrian noncurrency bullion coins as like-kind). Nonetheless, it may be possible to argue that two cryptocurrencies are similar enough to qualify as like-kind (for example, two mined cryptocurrencies on the same blockchain as opposed to a digital currency and a smart contract based token). As a result of the 2017 tax reform legislation,[80] however, Section 1031 can only apply to exchanges of real property, so like-kind exchanges of virtual currencies are no longer possible after 2017.

Treasury and the IRS have not issued any guidance concerning the appropriate treatment of a virtual currency hard fork. A fork is potentially analogous to a number of different kinds of transactions that are treated differently for tax purposes. As a result, the timing and character of any income that may be realized in connection with a fork or subsequent sale of virtual currency that is created by a fork is uncertain. In particular, it is not clear: (i) whether income is recognized at the time of the fork, at the time that a taxpayer exercises dominion and control over virtual currency created in the fork, or only at the time that a taxpayer sells or disposes of virtual currency; (ii) how dominion and control should be interpreted in the context of virtual currency created in a fork; (iii) how the basis in virtual currency created in a fork should be determined; and (iv) how the holding period of virtual currency created in a fork should be determined.

Treasury and the IRS have also not released guidance on the treatment of so-called "airdrops" of virtual currency or tokens—where holders of one digital token are given other digital tokens for free. The timing of income recognition in an airdrop is unclear, and airdrops may present valuation issues as well.

3. TAX TREATMENT OF TOKEN DISTRIBUTIONS AND SAFTS

Treasury and the IRS have not issued any guidance concerning the tax treatment of token distributions. In general, the facts and circumstances of a particular token distribution, including the nature of any rights associated with a token, must be analyzed to determine the appropriate characterization of the tokens for tax purposes. Depending on these facts, a token might properly be treated as convertible virtual currency under Notice 2014-21, as debt

80 Tax Cuts and Jobs Act, Pub. L. No. 115-97.

or equity interests in an entity established by the issuer, as equity in a de facto partnership among holders of the tokens, as a prepayment for goods and services, or as some other type of property. The tax consequences to issuers and holders of a particular token will depend upon this characterization of the token. In addition, token issuers may be subject to barter exchange reporting rules if the tokens are properly characterized as "scrip" through which clients of the issuer exchange property or services.

Some Token Sponsors pre-sell some amount of the digital tokens that the sponsor intends to distribute through a Simple Agreement for Future Tokens ("SAFT"). Under this model, the SAFT holder typically pays a fixed amount (usually in fiat currency or in a virtual currency) for the right to receive a determinable amount of tokens upon the occurrence of a "launch event," at which point the Token Sponsor distributes tokens. SAFTs typically provide that the intended tax treatment of the SAFT is as a forward contract. If this treatment is respected, then the issuance of the SAFT generally should not be a taxable event, and taxation of the purchase amount under the SAFT should be deferred until delivery of the tokens to the SAFT holder.

However, the characterization of a SAFT as a forward contract may not necessarily be respected by the IRS. For example, depending on the facts and circumstances, the IRS may seek to re-characterize a SAFT as a debt instrument or to distinguish a SAFT from a traditional prepaid forward contract and tax the proceeds upon receipt. The efficacy of the SAFT approach to token generation remains controversial, and is not a settled regulatory matter.

TOKEN ALLIANCE

CHAMBER OF DIGITAL COMMERCE

UNDERSTANDING DIGITAL TOKENS

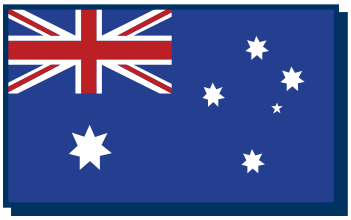
Legal Landscapes Governing Digital Tokens in Australia

Prepared by the Token Alliance – an industry initiative of the Chamber of Digital Commerce

FIRST EDITION • JULY 2018

II. PART 1: REGULATORY OVERVIEW OF DIGITAL TOKEN MARKETS

SECTION 4: AUSTRALIA



I. INTRODUCTION

The laws and regulations governing the securities and financial sectors in Australia are designed to ensure transparency and allow financial transactions to take place in a regulated and well-informed market. Protection of the consumer and participants in equity style transactions is paramount.

Token Sponsors in Australia operate in an evolving area of the law which currently sits on the periphery of regulations that apply to Australia's financial markets. To date, regulators have not taken steps to directly regulate the generation of digital tokens or crypto-assets. The current approach is to apply the securities and financial legal framework if the token has the characteristics of a security or financial product. If not, the token will be governed by existing consumer protection and general laws.

DIGITAL TOKENS MAY BE CLASSIFIED AS "FINANCIAL INSTRUMENTS" UNDER THE FOLLOWING:	
SECURITY	An interest that typically carries rights regarding the ownership of a company, voting rights in the decisions of a body and some entitlement to share in future profits.
MANAGED INVESTMENT SCHEME	When contributions from investors are pooled or used in common enterprise and participants do not have operational control over the scheme's management.
DERIVATIVE	An arrangement where the quantum of some required future consideration is determined by reference to an underlying asset.
NON-CASH PAYMENT FACILITY	An arrangement through which a person makes payments, or causes payments to be made, other than by physical delivery of money.
CROWDFUNDING	A method of raising small amounts of money from a large number of investors to finance a business.

In an attempt to deal with the increasing regulatory uncertainty surrounding digital tokens, the Australian Securities and Investments Commission ("ASIC"), the independent government body responsible for enforcing and regulating company and financial services laws in Australia, has issued a series of regulatory guidelines in the last 12 months setting out the factors in determining whether a token constitutes a security or a financial product. Importantly, if a token constitutes a security or a financial product, then the guidelines suggest that the token would be governed by existing securities legislation. Further, if the event creating, or mechanism to distribute, the tokens constituted a managed investment scheme, it would also be governed by existing securities legislation. In the event of uncertainty, ASIC also operates a service known as the Innovation Hub that allows industry to discuss regulatory issues with specialized personnel at ASIC to obtain clarity on compliance issues.

Unfortunately, apart from ASIC's regulatory guidelines and access to the Innovation Hub, there is no legal precedent and only limited literature on which a Token Sponsor may rely for clarification as to the applicability of existing law. Each token creation must be judged on its own facts and circumstances as to whether the token will constitute a security or financial product. However, ASIC has acknowledged that "crypto-assets and the use of distributed ledger technology has the potential to make an important contribution to fintech innovation,"[1] so it is hopeful that specific regulation will be introduced in the near future.

II. REGULATION OF DIGITAL TOKENS AND CRYPTO-ASSETS

The capital and financial markets in Australia are governed by various statutes that define and regulate securities, financial products, managed investment schemes, crowdfunding, and non-cash payment facilities. They also address events and circumstances that constitute deceptive and misleading conduct and impose sanctions and penalties for breach.

This report discusses the salient issues that may apply to digital tokens, crypto-assets, and Token Sponsors. Broadly, the relevant considerations relate to whether a digital token or crypto-asset will be classified as a security or financial product or whether the vehicle through which the token is generated constitutes a managed investment scheme.

A. WHAT IS A "SECURITY"?

"Securities" are defined in the *Corporations Act 2001* (Cth) ("Corporations Act") as including shares or debentures in a company, interests in a managed investment scheme or units of such shares and further includes legal or equitable rights or interests in the foregoing and options.[2]

"Shares" are generally regarded as an interest that carries rights regarding the ownership of a company, voting rights in the decisions of a body and some entitlement to share in future profits through dividends as well as a claim on the residual assets of a company if wound up.

1 Australian Securities & Investments Commission, 'Initial Coin Offerings And Crypto-Currency' *Information Sheet No 225* (May 2018) <http://asic.gov.au/regulatory-resources/digital-transformation/initial-coin-offerings/>.
2 *Corporations Act 2001* (Cth) s 92.

ASIC's approach to digital tokens is that if the purpose of the token is to fund a company, or if the bundle of rights attaching to the token are similar to rights commonly attaching to a share in a company, then it is likely that the token will fall within the definition of a share (security).[3] If so, the Token Sponsor must comply with the requirements of the Corporations Act in relation to the issue of securities, including the preparation of a prospectus, its registration with ASIC, and the necessary disclosures the prospectus must contain.

B. WHAT IS A "FINANCIAL PRODUCT"?

The Corporations Act provides both a general definition of "financial product," as well as a list of deemed financial products.

1. DEEMED FINANCIAL PRODUCTS

The list of deemed financial products includes securities (see above analysis), as well as derivatives and managed investment schemes.[4] ASIC has identified these deemed financial products as potential categories under which a digital token or crypto-asset may be captured.[5]

a. DERIVATIVES

In broad terms, a derivative involves an arrangement where the quantum of some required future consideration is determined by reference to some underlying asset, which may include a crypto-asset or digital token.[6] Recently, bitcoin futures contracts have become a popular investment and such a product is likely to be classified as a derivative under the Corporations Act.

b. MANAGED INVESTMENT SCHEME

Certain digital tokens or crypto-assets may fall under the umbrella of a Managed Investment Scheme ("MIS"). This is most likely the case when contributions from investors are pooled or used in common enterprise, and participants do not have operational control over the scheme's management.[7] Whether a digital token or crypto-asset constitutes a MIS will depend on the facts and circumstances, the assessment of which should include an assessment of what rights are attached to the tokens generated by the Token Sponsor. What constitutes a right should be interpreted broadly. These rights are likely to be set out in the Token Sponsor's white paper.

3 Australian Securities & Investments Commission, 'Initial Coin Offerings And Crypto-Currency' *Information Sheet No 225* (May 2018) <http://asic.gov.au/regulatory-resources/digital-transformation/initial-coin-offerings/>
4 *Corporations Act 2001* (Cth) s 764A(1).
5 Australian Securities & Investments Commission, 'Initial Coin Offerings And Crypto-Currency' *Information Sheet No 225* (May 2018) <http://asic.gov.au/regulatory-resources/digital-transformation/initial-coin-offerings/>.
6 *Corporations Act 2001* (Cth) s 761D.
7 *Corporations Act 2001* (Cth) s 9.

For example, payment for the purchase of a crypto-asset may be described as a receipt for a purchased service. However, if the value of the crypto-asset acquired is affected by the pooling of funds from investors or use of those funds under the arrangement, then the sale of the digital token may constitute a MIS. Use of a managed investment scheme triggers a range of product disclosure, licensing, and potential managed investment schemes registration obligations under the Corporations Act.[8]

New products may also be deemed to be financial products through regulations.[9] However, as of the date of this report, neither digital tokens nor crypto-assets have been designated as financial products. Importantly, ASIC has indicated that it does not consider bitcoin to be a financial product.[10]

2. THE GENERAL TEST FOR "FINANCIAL PRODUCTS"

"Financial product" is a term first introduced as part of financial services regulation reform in 2001. The term was intended to be sufficiently broad and flexible to allow emerging products to be captured under the regulation.

Importantly, the general test for what constitutes a financial product still applies to digital tokens and crypto-assets. Token Sponsors should consider all of the characteristics of the digital token or crypto-asset to determine whether it is a financial product at time of generation, or whether it may become a financial product after it is generated.

Section 763A(1) of the Corporations Act defines a financial product as a "facility through which, or through the acquisition of which, a person does one or more of the following:

a. MAKES A FINANCIAL INVESTMENT;

b. MANAGES FINANCIAL RISK; OR

c. MAKES NON-CASH PAYMENTS."

The financial investment limb is likely to be the most relevant for digital tokens and crypto-assets. Under the Corporations Act, a person makes a financial investment if:

a. "THE INVESTOR GIVES MONEY OR MONEY'S WORTH (THE CONTRIBUTION) TO ANOTHER PERSON AND ANY OF THE FOLLOWING APPLY:

i. the other person uses the contribution to generate a financial return, or other benefit, for the investor;

8 See broadly Australian Securities & Investments Commission, 'Offering Securities Under a Disclosure Document' *Regulatory Guidance No 254* (March 2016) <http://download.asic.gov.au/media/3578442/rg254-published-17-

9 Corporations Act 2001 (Cth) s 764A.

10 Australian Securities & Investments Commission, 'Initial Coin Offerings And Crypto-Currency' *Information Sheet No 225* (May 2018) <http://asic.gov.au/regulatory-resources/digital-transformation/initial-coin-offerings/>.

ii. the investor intends that the other person will use the contribution to generate a financial return, or other benefit, for the investor (even if no return or benefit is in fact generated);

iii. the other person intends that the contribution will be used to generate a financial return, or other benefit, for the investor (even if no return or benefit is in fact generated); and

b. THE INVESTOR HAS NO DAY-TO-DAY CONTROL OVER THE USE OF THE CONTRIBUTION TO GENERATE THE RETURN OR BENEFIT."[11]

ASIC has also made clear that simply describing a coin or token as a "utility" token or digital currency (in the relevant white paper or elsewhere) will not exclude it from being characterized as a financial product.[12] Instead, the Token Sponsor should assess the digital token or crypto-asset based on all of the rights and features associated with the product and obtain formal legal advice.

C. LICENSING REQUIREMENTS FOR FINANCIAL PRODUCTS

If a digital token or crypto-asset constitutes a financial product, the Token Sponsor may be required to obtain an Australian Financial Services License ("AFSL").[13]

Under Section 991A of the Corporations Act, "a person who carries on a financial services business… must hold an Australian financial services license covering the provision of the financial services." As the definition of "financial service" includes the issuing of a financial product,[14] issuers of applicable digital tokens and crypto-assets may fall within this requirement.

The process for applying for an AFSL includes providing substantial material to ASIC, employing or contracting with specialized staff to manage the provision of the relevant financial product and compliance generally, as well as the creation of compliance programs. The timeframe for obtaining an AFSL will vary depending on the circumstances of the application, but will typically require a number of months.

The need for an AFSL may be removed if one of the exemptions in Section 911A(2) of the Corporations Act applies. In particular, a product generator may not require an AFSL if:

a. THE PRODUCT IS OFFERED TO POTENTIAL INVESTORS THROUGH A THIRD PARTY WHO HOLDS AN AFSL WHICH COVERS THE GENERATION OF THAT PARTICULAR PRODUCT; AND

b. THE PRODUCT GENERATOR PROVIDES THE PRODUCT TO INVESTORS BASED ON THE OFFER PROPOSED BY THE THIRD PARTY LICENSEE.

Prohibitions on these kinds of outsourcing arrangements exist in particular circumstances, so Token Sponsors should evaluate the applicability of these exemptions on a case by case basis.

11 *Corporations Act 2001* (Cth) s 763B.
12 Ibid.
13 *Corporations Act 2001* (Cth) s 766C.
14 *Corporations Act 2001* (Cth) s 766A.

D. CROWDFUNDING

Raising funds by generating tokens can sometimes be considered a form of crowdfunding. If so, this activity will be covered by the crowd-sourced funding provisions of the Corporations Act.[15] It should be noted that crowd-sourced funding is regarded as a financial service. Accordingly, and in addition to compliance with the regulatory laws, an AFSL will be required to provide this service.

ASIC has warned Token Sponsors not to use the phrase 'crowd-sourced funding' unless the offering is in fact taking place under the crowd-sourced funding regime.[16] In addition, there is a $5 million cap on crowdfunding in Australia,[17] and the regime is currently only open to public unlisted companies.[18] However, amendments are currently being passed through the Parliament to open up the framework to proprietary companies, and there is a chance that these will be passed into law before the end of 2018.[19]

E. NON-CASH PAYMENT FACILITIES

Non-cash payment facilities are arrangements through which a person makes payments, or causes payments to be made, other than by physical delivery of money.[20] A typical example is a credit or debit card. If the token constitutes a non-cash payment facility, it will be governed by and must comply with the Corporations Act.

ASIC is presently of the view that, provided the token is more in the form of a gift card or utility token, it will not constitute a non-cash payment facility. [21]

F. DIGITAL TOKENS THAT ARE NOT FINANCIAL PRODUCTS

Even if digital tokens and crypto-assets (including bitcoin) are not regarded as securities or financial products, they must still comply with consumer law, contract law, and general Australian law.

One of the key laws that applies to all ICOs and crypto-assets (including those that are not financial products) is the general prohibition on parties engaging in misleading and deceptive conduct in the course of trade or commerce. Specifically, Section 18 of the Australian Consumer Law ("ACL") states that a person must not "in trade or commerce, engage in conduct that is misleading and deceptive or is likely to mislead or deceive." This prohibition has been extensively tested and developed through the courts and is considered a broad ranging prohibition.

15 See generally Part 6D.3A of the *Corporations Act 2001* (Cth).
16 Australian Securities & Investments Commission, 'Initial Coin Offerings And Crypto-Currency' *Information Sheet No 225* (May 2018) <http://asic.gov.au/regulatory-resources/digital-transformation/initial-coin-offerings/>.
17 *Corporations Act 2001* (Cth) s 738G.
18 *Corporations Act 2001* (Cth) s 738H.
19 Corporations Amendment (Crowd-sourced Funding for Proprietary Companies) Bill 2017.
20 *Corporations Act 2001* (Cth) s 763D.
21 Australian Securities & Investments Commission, 'Initial Coin Offerings And Crypto-Currency' *Information Sheet No 225* (May 2018) <http://asic.gov.au/regulatory-resources/digital-transformation/initial-coin-offerings/>.

ASIC has provided some guidance on potential conduct by a Token Sponsor that may be misleading or deceptive, including:

c. "the use of social media to generate the appearance of a greater level of public interest in a digital token or crypto-asset;

d. undertaking or arranging for a group to engage in trading strategies to generate the appearance of a greater level of buying and selling activity for a digital token or a crypto-asset;

e. failing to disclose adequate information about the Token Sponsor, the digital token, or the crypto asset, or

f. suggesting that the digital token or crypto-asset is a regulated product or the regulator has approved of the offering if that is not the case."[22]

A breach of this prohibition can result in serious penalties, including pecuniary penalties, for each instance of misleading and deceptive conduct.[23]

The power to enforce the prohibition on misleading and deceptive conduct in the area of digital tokens and crypto-assets has been specifically delegated to ASIC.[24] ASIC has also provided in depth information on this law in its latest guidance note,[25] so it is likely that this prohibition will be a key focus for the regulator when investigating Token Sponsors.

III. REGULATION OF DIGITAL CURRENCY EXCHANGES

In April 2018, new laws and policy principles were introduced to regulate the operation of Digital Currency Exchanges ("DCEs") in Australia. DCEs are businesses that exchange digital currency for fiat currency (*e.g.*, Dollars, Euros, RMB) and vice versa. The new laws require an entity to be enrolled and registered with the Australian Transaction Reports and Analysis Centre ("AUSTRAC") before operating as a DCE. All DCEs must also comply with obligations under the *Anti-Money Laundering and Counter-Terrorism Financing Act 2006* (Cth) ("AML/CTF Act") including the establishment and continued operation of a compliance program.

For those DCEs intending to offer exchange services for Token Sponsors in relation to digital tokens that are financial products, the DCE may also need a financial markets license or receive an exemption from ASIC in relation to their exchange services.

22 Ibid.
23 *Australian Consumer Law* ss 236, 237.
24 Australian Securities & Investments Commission, 'ASIC Takes Action On Misleading Or Deceptive Conduct In ICOs' (Media Release, 18-112MR, 1 May 2018) <https://asic.gov.au/about-asic/media-centre/find-a-media-release/2018-releases/18-122mr-asic-takes-action-on-misleading-or-deceptive-conduct-in-icos/>
25 Australian Securities & Investments Commission, 'Initial Coin Offerings And Crypto-Currency' *Information Sheet No 225* (May 2018) <http://asic.gov.au/regulatory-resources/digital-transformation/initial-coin-offerings/>

A. REGISTRATION OF DIGITAL CURRENCY EXCHANGES

The AML/CTF Act was amended in April 2018 to require DCEs to enroll and register their business with AUSTRAC before engaging in digital currency exchange services.[26] The amendments also set out the process for enrollment and registration, the establishment of the Digital Currency Exchange Register, and penalties for breaches of the registration requirements.

A set of policy principles and exemptions also came into effect in and around April 2018 stating that AUSTRAC will exercise leniency in relation to enforcement action until 2 October 2018.[27] During this time, AUSTRAC may only take enforcement action if a DCE fails to take reasonable steps to comply with the AML/CTF Act. Examples of 'reasonable steps' include:

a. complying with any breaches of the AML/CTF Act as soon as practicable;

b. implementing a transition plan outlining actions and timeframes to achieve compliance; and

c. allocating sufficient resources to enable compliance.[28]

Once the leniency period ends, it is likely that AUSTRAC will be diligent and prompt in pursuing enforcement action. The penalties that apply to breaches of the DCE obligations range from 2 to 7 years imprisonment and pecuniary penalties of $105,000 to $420,000.

B. PROCESS FOR ENROLLMENT AND REGISTRATION

A DCE can enroll and register with AUSTRAC using an online process based on the AUSTRAC business profile form.[29]

The DCE will need to provide certain information to AUSTRAC, including:

a. national police certificates and checks for certain personnel; and

b. certain information in relation to the business entity.

Foreign companies (whether or not they are registered in Australia) can apply for enrollment and registration. However, AUSTRAC requires the foreign company to provide certain information including any registration details, company history and details regarding any previous legal infringements.

26 AUSTRAC, 'Digital Currency Exchange Providers' *austrac.gov.au* (June 2018) <http://www.austrac.gov.au/digital-currency-exchange-providers/>

27 Anti-Money Laundering and Counter-Terrorism Financing (Digital Currency Exchange Register) Policy Principles 2018.

28 Ibid.

29 AUSTRAC, 'Enrollment and Registration' *austrac.gov.au* (April 2018) <http://www.austrac.gov.au/businesses/enrolment-and-registration/enrolment-and-registration>.

C. FINANCIAL MARKET LICENSE

Section 791A of the Corporations Act states that a person must only operate a financial market if:

a. the person has an Australian market license that authorizes the person to operate the market in this jurisdiction; or

b. the market is exempt.

This provision will be relevant to DCEs offering exchange services for digital tokens and crypto-assets constituting financial products. This is because a financial market is defined as "a facility through which:

a. offers to acquire or dispose of financial products are regularly made or accepted; or

b. offers or invitations are regularly made to acquire or dispose of financial products that are intended to result or may reasonably be expected to result, directly or indirectly, in:

   i. the making of offers to acquire or dispose of financial products; or

   ii. the acceptance of such offers."[30]

It is also important to note that a financial market may operate simultaneously in Australia and other jurisdictions. As such, DCEs that can be accessed in Australia but have been established outside of Australia may also need to obtain a financial markets license if the DCE offers to acquire or dispose of financial products are regularly made or accepted.

ASIC has also highlighted the financial market regulations and licensing requirements in its latest guidance note.[31] Due to the increased awareness of the financial markets license requirements, a number of DCEs operating in Australia have stopped listing new tokens and some DCEs have removed all tokens other than the mainstream tokens (bitcoin, Ethereum, and Ripple).

Even if a financial markets license is required to operate a DCE, such activity may be exempted by Ministerial power for a particular financial market or a class of financial markets.[32] As of the date of this report, no exemption has been given for a financial market for digital tokens and crypto-assets.

30 *Corporations Act 2001* (Cth) s 767A.
31 Australian Securities & Investments Commission, 'Initial Coin Offerings And Crypto-Currency' *Information Sheet No 225* (May 2018) <http://asic.gov.au/regulatory-resources/digital-transformation/initial-coin-offerings/>.
32 *Corporations Act 2001* (Cth) s 791C.

IV. ASIC'S INNOVATION HUB AND REGULATORY SANDBOX

In an effort to allow regulation to follow rather than restrain innovation and change in the FinTech markets, ASIC has developed programs and tools to assist industry in Australia with navigating the regulatory environment and foster the creation of crypto-asset businesses.

In March 2015, ASIC launched the Innovation Hub, an initiative to help fintech businesses navigate the regulatory system in the financial services sector. The main service provided by the Innovation Hub is direct access to senior staff at ASIC to streamline licensing and offer informal guidance in relation to the regulatory requirements for the business.[33] Since its inception, the Innovation Hub has assisted in the granting of over 36 licenses to FinTech businesses and these businesses received their licenses much faster than those applying through the standard process.[34] Recently, the Innovation Hub has focused on digital tokens and crypto-assets and members of the Innovation Hub are key contributors to the regulatory guidelines that have been issued by ASIC.

As part of the Innovation Hub initiative, ASIC established a licensing relief framework dubbed the ASIC "regulatory sandbox" allowing users to work cooperatively with ASIC on regulatory issues to achieve a solution that suits both the relevant firm and government.[35]

The sandbox comprises the following three relief options:

a. assistance to identify existing statutory exemptions or flexibility;

b. relief for testing certain specified products and services; or

c. for other services, where ASIC grants individual relief.[36]

The sandbox may be used by new-to-market Token Sponsors to liaise with ASIC to determine whether their token would be considered a financial product. However, the sandbox is not available for testing the issuance of financial products (including any digital tokens or crypto-assets considered financial products).[37]

33 Australian Securities & Investments Commission, 'ASIC's Innovation Hub And Our Approach To Regulatory Technology' *Report 523* (May 2017) <https://asic.gov.au/regulatory-resources/find-a-document/reports/rep-523-asic-s-innovation-hub-and-our-approach-to-regulatory-technology/>.

34 Commissioner John Price, 'The Fintech Sector Opportunity: ASIC's Perspective'(Speech delivered at the 4th Annual Fintech Summit 2017, Sydney, Australia, 2 November 2017).

35 Australian Securities & Investments Commission, 'ASIC Releases World-First Licensing Exemption For Fintech Businesses' (Media Release, 16-440MR, 15 December 2016) <https://asic.gov.au/about-asic/media-centre/find-a-media-release/2016-releases/16-440mr-asic-releases-world-first-licensing-exemption-for-fintech-businesses/>

36 Australian Securities & Investments Commission, 'Testing Fintech Products And Services Without Holding An AFS Or Credit License' *Regulatory Guide No 257* (August 2017) <https://asic.gov.au/regulatory-resources/find-a-document/regulatory-guides/rg-257-testing-fintech-products-and-services-without-holding-an-afs-or-credit-licence/>.

37 Ibid.

VI. TAXATION

The tax treatment of Token Sponsors remains a pressing issue relative to both the classification of the digital token as either belonging to the capital or revenue account, and the uncertain applicability of the goods and services tax ("GST").

For digital tokens that are caught by the existing financial product or securities regimes, the tax treatment is relatively settled, with significant bodies of law, including statute, case law, and guidance from the Australian Taxation Office ("ATO"), clarifying the tax treatment of securities and financial products. However, for those tokens that sit outside of the existing regulatory frameworks, the tax treatment is unclear.

If a digital token is not a regulated security or financial product, its sale will likely be treated as revenue of the Token Sponsor and taxed accordingly at the corporate tax rate. There is currently significant discussion in Australia around the granting of deferred taxation liability for Token Sponsors, in recognition of the fact that the funds raised by most Token Sponsors are often allocated to a roadmap stretching years into the future. However, no amendments have yet been suggested to the existing law.

The ATO has repeatedly stated that the tax treatment of Token Sponsors will turn upon the facts and circumstances of the triggering event. Accordingly, many Australian Token Sponsors have taken the path of seeking a private ruling from the ATO to clarify their tax position. While these private rulings will be released by the ATO in redacted form, they may not be relied upon by third parties. In any event, as at the time of writing, no private rulings have been handed down by the ATO in relation to Token Sponsors, despite many currently being underway.

The GST treatment of tokens remains contentious. Prior to 1 July 2017, GST was payable in relation to sales and purchases of "digital currency." From 1 July 2017, these activities were specifically exempted from the GST regime. While the ATO has expressly recognized that bitcoin, Ethereum, Litecoin, Dash, Monero, Zcash, Ripple, and Ybcoin fall within the definition of "digital currency,"[38] the definition is relatively narrow. Guidance from the ATO released in March 2018 clarifies that Australian Token Sponsors, as well as foreign Token Sponsors selling into the Australian market, may still be required to pay GST on their offerings, particularly where the token provides a right or entitlement to goods or services.[39]

VII. CONCLUSION

Overall, both Australian Token Sponsors and foreign Token Sponsors maintaining a presence within the Australian market are currently operating in an uncertain legal environment. The Australian regulators, like almost all of the regulators in other jurisdictions discussed in this report, have adopted an approach based on functional equivalence. Where a digital token or crypto-asset falls within the existing

38 Australian Taxation Office, 'GST And Digital Currency' ato.gov.au (March 2018) <https://www.ato.gov.au/Business/GST/In-detail/Your-industry/Financial-services-and-insurance/GST-and-digital-currency/>.
39 Ibid.

framework, the answer is clear. However, the majority of digital tokens do not easily fit within existing frameworks. The result is less than optimal both for regulators and Token Sponsors on the one hand and the general public on the other. Industry groups, including the Australian Digital Commerce Association,[40] have recognized that clearer guidelines and principles are required. Best practice guidelines are currently being drafted in the expectation that industry will embrace and adhere to these in the hope that they will form the basis for future regulation.

Ultimately, activity from Token Sponsors will continue to grow in Australia as clear economic and technical drivers accelerate market activity. It is hoped that this report encourages regulatory activity to grow as well.

40 For more information on the Australian Digital Commerce Association, see https://adca.asn.au/.

TOKEN ALLIANCE

CHAMBER OF DIGITAL COMMERCE

UNDERSTANDING DIGITAL TOKENS

Legal Landscapes Governing Digital Tokens in Canada

Prepared by the Token Alliance – an industry initiative of the Chamber of Digital Commerce

FIRST EDITION • JULY 2018

II. PART 1: REGULATORY OVERVIEW OF DIGITAL TOKEN MARKETS

SECTION 2: CANADA

I. INTRODUCTION

Digital token units, often referred to as "coins" or "tokens", issued as part of an ICO or initial token offering ("ITO") – terms for digital token distributions that have been used by Canadian Securities Administrators – can represent many different things, including a portion of an asset, whether tangible or intangible; services or units of services; or an ownership interest in a business. Whether Canadian securities laws apply to ICOs and ITOs will likely depend on the use to which the coin or token may be put and what rights it represents.

There may be a distinction between tokens that fall within the ambit of securities regulation and those that fall outside of it. Proponents of this view conceive of at least two distinct types of tokens. The concept of a "utility token" involves a token or coin that represents services or units of services, for example, using tokens to play a game at an arcade. On the other hand, a "securities token" entitles the holder of the token or coin to certain rights in the business' assets, revenues or profits. Since a securities token functions similar to a typical security such as a share, Canadian securities laws are likely to apply.

While reference is made throughout this discussion to "securities tokens," it is important to note that any distinction between utility tokens and securities tokens has not been explicitly accepted by Canadian securities regulatory authorities. On August 24, 2017, Canadian Securities Administrators ("CSA") staff, with the exception of Saskatchewan, published Staff Notice 46-307 – *Cryptocurrency Offerings*[1] ("CSAN

1 Canadian Securities Administrators, *CSA Staff Notice 46-307 Cryptocurrency Offerings* (Toronto: Ontario Securities Commission, 2017), online: http://www.osc.gov.on.ca/en/SecuritiesLaw_csa_20170824_cryptocurrency-offerings.htm.

46-307"), in response to requests from fintech businesses for guidance on the applicability of Canadian securities laws to "cryptocurrency offerings," "cryptocurrency exchanges," and "cryptocurrency-focused investment funds." CSAN 46-307 articulated a general view that "in many instances" digital tokens associated with ICOs/ITOs are securities.

On June 11, 2018, the CSA published Staff Notice 46-308 *Securities Law Implications for Offerings of Tokens*[2] ("CSAN 46-308"), which provides additional guidance on the applicability of securities law to offerings of blockchain-based tokens or coins.

The discussion that follows outlines certain of the Canadian securities law considerations that may apply to the distribution or trading of a digital token that qualifies as a "security" within the meaning of Canadian securities laws.

II. THE CANADIAN LEGAL FRAMEWORK

Securities legislation in Canada is principally governed by Canada's ten provincial and three territorial governments with the view of balancing investor protection against efficient capital markets.[3] While each province and territory has its own securities legislation, some coordination among jurisdictions is achieved through the CSA as an umbrella organization.[4] While the following discussion will focus mainly on the securities laws of the Province of Ontario, the rules in many areas of securities regulation have been standardized among the provinces and territories and cooperative systems have been established among the regulators through the CSA.

A. THE DEFINITION OF "SECURITY" AND ITS APPLICATION TO DIGITAL TOKENS

The provincial securities Acts have expansive statutory definitions of "security."[5] The statutory definitions of "security" include as one category, an "investment contract", which is the category Canadian courts and securities regulators generally use to assess whether a new type of transaction involves a security.

The leading case in Canadian jurisprudence on the meaning of investment contracts is *Pacific Coast Coin Exchange v. Ontario Securities Commission*[6] ("Pacific Coast"), which was expressly cited as the relevant case law in CSAN 46-307. The Supreme Court of Canada in Pacific Coast considered and adopted certain United States jurisprudence on the meaning of investment contracts, and in particular, the common law test set out in *SEC v. W.J. Howey Co.*, 328 U.S. 293 (1946) and other United States cases.

2 Canadian Securities Administrators, CSA Staff Notice 46-308 Securities Law Implications for Offerings of Tokens (Toronto: Ontario Securities Commission, 2018), online: http://www.osc.gov.on.ca/en/SecuritiesLaw_csa_20180611_46-308_securities-law-implications-for-offerings-of-tokens.htm
3 *See* section 1.1 ("Purposes of Act") of Ontario's Securities Act R.S.O. 1990, c. S.5.
4 Canadian Securities Administrators, online: https://www.securities-administrators.ca/.
5 *See, e.g.*, section 1(1) of the Ontario *Securities Act* R.S.O. 1990, c. S.5 for the definition of "security."
6 *Pacific Coast Coin Exchange v. Ontario Securities Commission*, [1978] 2 S.C.R. 112.

The application of this Canadian case law to so-called "utility" tokens has not been further elaborated upon directly by the Canadian courts.

In its application to "cryptocurrency offerings," the CSA has stated that it will conduct an evaluation of whether a "cryptocurrency" – a term that it leaves undefined – qualifies as a "security" on a case-by-case basis and that substance will be considered over form. In CSAN 46-307, the CSA noted that the appropriate interpretive test was the four-prong test: does the ICO/ITO involve (1) an investment of money, (2) in a common enterprise, (3) with the expectation of profit, (4) to come significantly from the efforts of others. The CSA further stated in CSAN 46-307 that the case law requires an assessment of the economic realities of a transaction and a purposive interpretation, keeping in mind the objective of investor protection.[7]

The CSA did not provide any clear guidance in CSAN 46-307 on the characteristics that would indicate that "securities may not be involved." Generally, however, it can be concluded that a token that entitles the holder to share in the business profits of the entity distributing the token will likely be considered a security.

In CSAN 46-308, the CSA emphasized that one should assess not only the technical characteristics of the token itself, but the economic realities of the offering as a whole, with a focus on substance over form. With respect to utility tokens, CSAN 46-308 noted that, "the fact that a token has a utility is not, on its own, determinative as to whether an offering involves the distribution of a security."

CSAN 46-308 provided additional guidance on how the CSA staff have viewed certain examples, based on situations seen to date. The anonymized examples focused on various elements of the *Howey* test.

In CSAN 46-308, the CSA staff expressed the view that if management "clearly and uniformly promotes the token in a manner that, taken as a whole, promotes only its utility and not its investment value, the implication that purchasers have an expectation of profit may be reduced."

If tokens are not fungible or interchangeable and each token has unique characteristics, and any future market value of the token is primarily based on market forces, the value of the token may be based on its unique characteristics, and not on the efforts of others. There may not be a common enterprise.

If tokens have a fixed value on the platform that does not automatically increase over time, or change based on non-commercial factors, this may reduce the purchaser's expectation of profit.

If the token's software, platform or services are not yet available or are still in development, the CSA said this could indicate that the purchaser is not purchasing the tokens for their immediate utility, but because of an expectation of profit. "Although some purchasers may be purchasing the token for

7 *Canadian Securities Administrators, supra* note 83.

the utility function, many purchasers may be purchasing the token in order to sell it on a cryptoasset trading platform or otherwise in the secondary market." This is particularly true where the existence of secondary trading is critical to the success of the offering of tokens or is featured prominently in the marketing of the offering. This could also indicate the existence of a common enterprise because management's efforts are still needed to develop or deliver the software, online platform or application or goods and services.

B. CSA SANDBOX APPROVALS

The CSA established a regulatory sandbox[8] in February 2017 (the "CSA Sandbox"), a program whereby issuers seeking to offer innovative products, services and applications, such as digital tokens, are invited by the CSA to discuss their business model and applicable securities laws, and possible exemptive relief, directly with the applicable securities regulators on a coordinated and flexible basis. As CSA Sandbox approvals are intended to allow the issuers to operate in a test environment, the approvals are time-limited, so far to one or two years.

To date, only two limited exemptions relating to digital tokens have been granted through the CSA Sandbox process.

The first limited exemption was for Montreal-based Impak Finance Inc. ("Impak"), which received exemptive relief on August 16, 2017 from the Québec Autorité des marchés financiers ("AMF") and seven other Canadian jurisdictions from the dealer registration requirement and the prospectus requirement in respect of the resale of Impak Coins ("MPK").[9] The initial distribution of MPK was made in accordance with the standard terms of an already existing statutory offering memorandum prospectus exemption. This allowed Impak to carry out the ICO. The issuance of MPK, a new digital currency based on the Waves blockchain platform, was proposed in order to fund the development of Impak's online social network dedicated to the impact economy. The MPK network did not exist at the time of the ICO. MPK were not delivered to purchasers upon closing of the offering, rather, only once Impak launches its digital wallet sometime in the future.

DIGITAL TOKEN PRODUCTS RECEIVING EXEMPTIVE RELIEF IN THE CSA REGULATORY SANDBOX

COMPANY	PURPOSE OF SANDBOX TRIAL
IMPAK	Issue MPK tokens to fund the development of Impak's online social network, impak.eco.
TOKEN FUNDER	Offer FNDR Tokens on the Ethereum blockchain to investors to fund the creation of Token Funder's smart token asset management platform, intended to facilitate third-party issuers raising capital through the offering of blockchain-based securities.

8 Canadian Securities Administrators, *CSA Regulatory Sandbox* (Montreal: Canadian Securities Administrators, 2017) online: https://www.securities-administrators.ca/industry_resources.aspx?id=1588.

9 *Re Impak Finance Inc.* (16 August 2017), online: http://www.osc.gov.on.ca/en/SecuritiesLaw_ord_20170921_215_impak.htm.

The Impak exemption order had a number of significant conditions. Impak was required to conduct both know-your-client and suitability reviews for each MPK purchaser. In this context KYC means more than simply identity verification, and includes knowing clients' overall investment experience and objectives, in order to assess investment suitability for the client. Impak was permitted to accomplish this through an online interactive questionnaire. There was no prospectus relief granted for any resale by a holder of MPK, except for a transfer by a participant to a social impact merchant. MPK cannot be listed and traded on any exchange unless it is done in accordance with Canadian securities laws and first approved by the AMF. The exchange rate for MPK to the Canadian dollar is established by an MPK governance body, and MPK may be redeemed for Canadian dollars at that rate, although Impak does not guarantee the purchase or conversion of MPK to participants. The exemption expires 24 months from the date of the decision.

The second limited exemption was for Toronto-based Token Funder Inc. ("Token Funder"), which received exemptive relief on October 17, 2017 from the Ontario Securities Commission ("OSC") and other Canadian securities regulators from the dealer registration requirement to allow it to sell its own digital tokens, called FNDR Tokens, to the public.[10] The initial distribution of FNDR Tokens would be made in accordance with the standard terms of an already existing statutory offering memorandum prospectus exemption. Token Funder was seeking to offer FNDR Tokens on the Ethereum blockchain to investors in order to fund the creation of its smart token asset management platform, intended to facilitate third-party issuers raising capital through the offering of blockchain-based securities. FNDR Tokens were designed to share in distributions from Token Funder arising from the operation of the platform, in the discretion of the Board of Directors of Token Funder and will have certain voting rights on the entities entitled to use the platform. FNDR Tokens cannot be listed and traded on any exchange unless done in accordance with Canadian securities laws and first approved by the OSC. The exemption will expire 12 months from the date of the decision.

Unlike the FNDR Tokens, MPK was unusual in that it was generally not freely transferable by its terms, but was redeemable at a non-guaranteed rate to be established. Given that the Impak network was still a work in progress, the MPK tokens had no utility at the time of the ICO and were treated by the issuer and the AMF as being investment contracts. The FNDR Tokens are more clearly securities tokens due to their distribution entitlements. From these two narrow examples, few clear factors on the broader application of the law around investment contracts to tokens can be elucidated.

C. FACTORS RELATING TO THE CONSIDERATION OF WHETHER A TOKEN IS A SECURITY

While the following factors are relevant to the analysis of whether a token does or does not qualify as a "security," it is not clear whether the securities regulatory authorities in Canada will consider any particular factor or set of factors as determinative:

10 *Re Token Funder Inc.* (17 October 2017), online: http://www.osc.gov.on.ca/en/SecuritiesLaw_ord_20171023_token.htm.

- What is the token's use or purpose?
- Does the token represent access to a business' platform, or does it represent an ownership stake in a business that could increase or decrease in value depending on the success of the business?
- At the intended time of sale of the token, does the relevant platform still need to be developed or is there an existing, functioning ecosystem in which the token can be utilized?
- Will the purchaser receive the token upon payment of the full price?
- Is the token's market value reflective of the general attractiveness of the business?
- Is the token transferable, and is the anticipated value derived from future market demand?
- Does the token expire after a certain period of time of not being in use?
- Is the purchaser's purpose for purchasing the token personal use or consumption, rather than merely investment purposes?

III. CONSIDERATIONS REGARDING "ICOS" OF A "SECURITY"

A. ISSUING A SECURITIES TOKEN

1. PROSPECTUS REQUIREMENT OR EXEMPTION

If the purchaser of a securities token is located in a Canadian jurisdiction, Canadian securities laws must be considered regardless of the location of the issuer of the token. Canada's prospectus requirement creates a closed-system whereby any distribution of a security, even if made by a private company, must either be qualified by a prospectus or must qualify for a prescribed prospectus exemption.

To date, there has been no prospectus filed and approved to undertake an ICO in Canada. Upon filing and receiving a receipt for a final prospectus, the issuer would become a "reporting issuer" in Canada. A reporting issuer is subject to all of the continuous and timely disclosure requirements of Canadian securities laws, which are extensive and include the requirement to prepare and disseminate quarterly and audited annual financial statements.

As an alternative to a public prospectus, one of the most commonly used prospectus exemptions is the "accredited investor" exemption.[11] This exempts an issuer or selling security holder from the prospectus requirement when distributing securities to certain institutional investors or wealthy individuals (for example an individual whose financial assets before taxes but net of liabilities of over $1 million, or whose net income exceeds $200,000 in each of

11 Section 2.3 of National Instrument 45-106 — *Prospectus Exemptions*.

the two most recent calendar years).[12] Individual accredited investors below certain financial thresholds are required to receive and sign a prescribed risk acknowledgment form.

Token Funder and Impak each relied on the "offering memorandum" prospectus exemption[13] in respect of the initial distribution of their securities tokens. While the details vary by Canadian jurisdiction, the offering memorandum exemption allows an issuer to distribute its securities to purchasers who are not accredited investors or eligible investors (which are investors who meet a slightly less stringent financial test than the accredited investor test), so long as the issuer provides purchasers with a prescribed form of offering memorandum (which is similar to a prospectus), the issuer obtains a signed risk acknowledgment form from the purchaser and the purchaser's acquisition cost does not exceed a prescribed maximum amount. While the prescribed maximum amount in many jurisdictions is ordinarily $10,000 for non-eligible investors, the OSC and the AMF in their exemptive relief decisions in respect of Token Funder and Impak, imposed lower $2,500 investment limits for investors who did not qualify as accredited investors or eligible investors.

2. MARKETING RESTRICTIONS

"Trading" of securities includes any act, advertisement, solicitation, conduct or negotiation directly or indirectly in furtherance of a distribution of securities, and thus triggers the prospectus requirement.[14]

If the accredited investor exemption is to be relied upon, before a marketing document, such as a term sheet or offering memorandum, is provided to potential investors, their eligibility for the accredited investor exemption must already have been assessed. In the case of reliance on the offering memorandum exemption, an offering memorandum in the prescribed form and in many cases, a risk acknowledgment form, must be obtained from the purchaser prior to signing the agreement to purchase the security.

In order to meet these requirements, issuers have used a "walled garden" approach whereby potential investors may access the electronic marketing materials on the issuer's website only once their compliance with the applicable exemption has been verified.

3. EXEMPT DISTRIBUTION REPORTING

Certain prospectus exemptions, including the accredited investor and offering memorandum exemptions, require the filing of exempt distribution reports (and in some cases offering memoranda) with the CSA within ten days after the distribution.[15] The names of any agents or underwriters that assist with an offering of securities tokens and their fees must also be

12 Ontario Securities Commission, *Summary of Key Capital Raising Prospectus Exemptions in Ontario* (Toronto: Ontario Securities Commission, 2016), online: http://www.osc.gov.on.ca/en/SecuritiesLaw_ni_20160128_45-106_key-capital-prospectus-exemptions.htm.
13 Section 2.9 of National Instrument 45-106 — *Prospectus Exemptions*.
14 *See, e.g.*, the definition of "trade" under section 1(1) of the Ontario *Securities Act* R.S.O. 1990, c. S.5.
15 *See, e.g.*, Form 45-106F1 *Report of Exempt Distribution* (Form 45-106F1).

recorded on the reports. As these exempt distribution reports require detailed information about purchasers, issuers of securities tokens must ensure their purchase procedures have the capability of capturing and recording information in respect of each purchase of securities, including the name, address and telephone number of each investor in Canada, their particular sub-category of accredited investor, if applicable, as well as the price and number of securities purchased by each investor. Issuers based in the Canadian provinces of Alberta, British Columbia or Québec have additional reporting obligations, even for distributions made outside Canada.

4. RESALE RESTRICTIONS

Securities tokens purchased in reliance upon a prospectus exemption are subject to restrictions on resale pursuant to National Instrument 45-102 – *Resale of Securities* ("NI 45-102"). NI 45-102 generally prohibits resale of a security purchased under the accredited investor exemption unless either (i) the issuer of the security has been a reporting issuer in a jurisdiction of Canada for the four months preceding the trade, or (ii) the resale is made under another prospectus exemption, such as the accredited investor exemption, which would entail continued resale restrictions, or the security is of a foreign issuer and is resold outside Canada under certain conditions.[16] Unless the issuer of a securities token becomes a reporting issuer in Canada, the resale restrictions continue indefinitely and do not expire, so the tokens would never become freely tradeable in Canada.

B. TRADING OR ADVISING IN SECURITIES TOKENS

Persons in the business of trading or advising in securities, or holding themselves out as being in the business of trading or advising in securities, must register as dealers or advisers with the relevant CSA regulator and meet the requirements set out in National Instrument 31-103 – *Registration Requirements, Exemptions and Ongoing Registrant Obligations*.[17] The determination of whether one is, or holds oneself out to be, in the business of trading or advising in securities is a factual determination commonly referred to as the "business trigger" for registration.

Startup issuers that are raising capital to advance their operating business plans would typically not be considered to be in the business of trading in securities unless they engage an employee with primary responsibility and/or compensation for capital raising activities. However, it is notable that both Token Funder[18] and Impak[19] sought and received temporary exemptions from the dealer registration requirement upon conditions, including: conducting investment know-your-client and suitability reviews of purchasers, not providing investment advice to purchasers, and establishing

16 Resale of Securities, OSC NI 45-102 (30 April 2016), online: https://www.osc.gov.on.ca/documents/en/Securities-Category4/rule_20170119_45-102_unofficial-consolidation.pdf.
17 *Registration Requirements, Exemptions and Ongoing Registrant Obligations*, OSC NI 31-103 (11 January 2015), online: http://www.osc.gov.on.ca/documents/en/Securities-Category3/ni_20150111_31-103_unofficial-consolidated.pdf.
18 *Ontario Securities Commission, supra* note 92.
19 *Ontario Securities Commission, supra* note 91.

policies and procedures that establish a system of controls and supervision sufficient to manage the risks of the business.

On September 6, 2017, Canada's first "Cryptocurrency Fund," a term used by the CSA to refer to an investment fund that invests solely in specified digital tokens, was established. The British Columbia Securities Commission ("BCSC") and the OSC granted to First Block Capital Inc. ("First Block") the first registration in Canada to an investment fund manager ("IFM") and exempt market dealer ("EMD") solely dedicated to digital token investments, in order to operate a bitcoin investment fund.[20] First Block's registration was granted subject to a number of tight restrictions and requirements, including:[21]

- Prior approval must be granted by the BCSC for any new Cryptocurrency Fund established by First Block;
- A specific custodian (Xapo) was prescribed and changes to a Cryptocurrency Fund's custodian or to the entity principally responsible for the execution of trades for such fund will also be subject to prior approval;
- First Block must require its custodians and brokers to maintain compliance systems that provide reasonable assurance of compliance with regulatory requirements, and to manage business risks in accordance with prudent business practices;
- Independent auditor reports reviewing the sufficiency of the Cryptocurrency Fund's custodian's security practices as well as regulatory compliance documents received by First Block from its custodians and brokers must be provided to the BCSC;
- Annual audited financial statements must be available to security holders for each Cryptocurrency Fund, and net asset value reports must be available on a monthly or more frequent basis for each Cryptocurrency Fund; and
- Prior to making a trade in a digital token, First Block must make its own determination of a current and reasonable fair price for the digital token.

Subsequently, the Alberta Securities Commission ("ASC"), OSC and AMF imposed similar restrictions on the registrations of Ross Smith Asset Management ULC ("RSAM"),[22] 3iQ Corp.,[23] and Majestic Asset Management LLC ("Majestic"),[24] respectively, each of which notified the relevant regulator

20 British Columbia Securities Commission, *B.C. Securities Commission grants landmark Bitcoin investment fund manager registration* (Vancouver: British Columbia Securities Commission, 2017), online: https://www.bcsc.bc.ca/News/News_Releases/2017/69_B_C__Securities_Commission_grants_landmark_bitcoin_investment_fund_manager_registration/.

21 First Block Capital Inc. (5 September 2017), online: https://www.securities-administrators.ca/uploadedFiles/Industry_Resources/DE_First%20Block.pdf.

22 *Ross Smith Asset Management ULC* (22 September 2017), online: https://www.securities-administrators.ca/uploadedFiles/Industry_Resources/TC_RossSmith.pdf.

23 3iQ Corp. (19 January 2018), online : https://www.securities-administrators.ca/uploadedFiles/Industry_Resources/TC_3iQ%20Corp_ProposedOntariotermsandconditions.pdf.

24 *Majestic Asset Management LLC* (26 January 2018), online: https://www.securities-administrators.ca/uploadedFiles/Industry_Resources/TC_MajesticEn_2018-01-25.pdf

that it intended to establish, manage and distribute securities of a fund that will invest solely in "cryptocurrencies," which, for the purposes of the decision documents, the ASC, OSC, and AMF (as applicable) defined to mean bitcoin, ether, Litecoin (in the case of the 3iQ Corp. decision document) and "anything commonly considered a cryptocurrency, digital or virtual currency, or digital or virtual token."[25] The decision documents note that an investment fund that invests solely in one or more specified "cryptocurrencies" is a novel business model in Canada and, as such, additional reporting is required in order to monitor developments in the area.

It was significant at the time that First Block was not also required to register as a portfolio manager in order to manage investment activity for the initial bitcoin trust, as this implied that the underlying bitcoin was not considered by the BCSC and OSC to be a security. However, RSAM, 3iQ Corp., Majestic and Rivemont Investments Inc., investment portfolio manager of the fund created by Majestic, are all also registered as portfolio managers, implying that the issue is not yet settled.

On December 5, 2017, the OSC issued a notice to all registered firms (dealers, advisers or investment fund managers) saying that any firms that plan to establish, manage, advise and/or trade in securities of investment funds with portfolios of "[b]itcoin and/or other cryptocurrencies, cryptocurrency assets and coins and token offerings" are required to report changes in their business activities "to include cryptocurrency products and/or services" by completing and filing a prescribed form of notice of change of registration information.[26] The OSC said that following reviews of the information provided, the OSC may impose terms and conditions on the firm's registration to ensure adequate investor protection.[27]

C. CREATING A MARKET FOR SECURITIES TOKENS

As part of CSAN 46-307, the CSA signaled its concern that platforms facilitating trades in coins, tokens or cryptocurrencies that qualify as securities may also be subject to Canadian securities law requirements involving recognition or exemption from recognition as an exchange or as a quotation and trade reporting system.[28] At this point in time, no entity has obtained the recognition required, nor an exemption from such recognition requirement, in order to allow Canadians to participate in on-exchange trading of tokens that are securities.

The definition of "marketplace" in the Ontario *Securities Act* and other relevant rules is broad and includes an exchange, a quotation and trade reporting system, or any person or company that constitutes, maintains or provides a market or facility for bringing together orders for securities from

25 *3iQ Corp., supra* note 105.
26 Ontario Securities Commission, *Form 33-109F5 requirement for registered firms that establish, manage, advise and/or trade in securities of cryptocurrency investment funds* (Toronto: Ontario Securities Commission, 2017), online: http://www.osc.gov.on.ca/en/Dealers_eb_20171205_registered-firms-33-109.htm.
27 *Id*
28 *Canadian Securities Administrators, supra* note 83.

multiple buyers and sellers using established, non-discretionary methods under which orders interact with each other and the buyers and sellers entering into the orders agree to the terms of a trade.[29]

A person or company is considered to bring together orders for securities if it (a) displays, or otherwise represents to marketplace participants, trading interests entered on the system; or (b) receives orders centrally for processing and execution. Merely routing orders to marketplace or a dealer for execution is not considered to be providing a market or facilities for bringing together buyers and sellers of securities.[30]

Marketplaces will generally be found to be exchanges if the marketplace provides a listing function, provides a guarantee of a two-sided market for a security on a continuous or reasonably continuous basis, sets requirements governing the conduct of marketplace participants or disciplines marketplace participants, for example by levying fines or taking enforcement action.[31] A marketplace that does not meet these exchange indicia and is not a quotation and trade reporting system may be characterized as an "alternative trading system" ("ATS"). An ATS proposing to carry on business in Canada is required to become registered as an investment dealer and provide detailed specified information to the CSA.

IV. ANTI-MONEY LAUNDERING

In 2014, the federal government proposed amendments to the Proceeds of Crime (Money Laundering) and Terrorist Financing Act ("PC Act")[32] that, once in force, will require entities engaged in the business of "dealing in virtual currencies" to register as money services businesses with the Financial Transactions and Reports Analysis Centre ("FINTRAC"). In June 2018 the Department of Finance published proposed regulations defining what "virtual currency" means. In that regard virtual currency is defined as (a) a digital currency that is not fiat currency and that can be readily exchanged for funds or for another virtual currency that can be readily exchanged for funds; or (b) information that enables a person or entity to have access to a digital currency referred to in paragraph (a). The proposed regulations would limit AML/ATF obligations to virtual currencies that are exchangeable, also known as convertible. This would include both centralized virtual currencies which are administered by a single authority and decentralized virtual currencies such as bitcoin, where authority is distributed across a network. The definition of virtual currency also includes information that provides access to the use of virtual currency, such as a private key in a cryptographic key pairing. There is a comment period in respect to the proposed regulations until September 7, 2018, and accordingly the final language will not be finalized until after that time. The proposed amendments to the PC Act have already received Royal Assent but the in-force date is not known.

29 *See* section 1(1) of the Ontario *Securities Act* R.S.O. 1990, c. S.5 for the definition of marketplace.
30 *See* section 2.1(3) of *Marketplace Operation*, OSC NI 21-101 (1 January 2015).
31 Ontario Securities Commission, *Exchanges* (Toronto: Ontario Securities Commission, 2018), online: http://www.osc.gov.on.ca/en/Marketplaces_exchanges_index.htm.
32 *Proceeds of Crime (Money Laundering) and Terrorist Financing Act* S.C. 2000, c. 17.

Once the proposed amendments are in force, entities that must register as money services business will need to report certain transactions to FINTRAC, verify the identities of customers and maintain records with respect to transactions beyond a financial threshold and implement an anti-money laundering and counter-terrorist financing compliance regime. These requirements will apply to entities that have a place of business in Canada as well as entities that do not, provided they direct their services to persons or entities in Canada. As they are drafted, the proposed amendments will not apply to entities or individuals that simply use, and do not otherwise deal in, digital tokens.

Until the proposed amendments are in force, platforms that trade digital tokens that are not securities are not directly addressed in the PC Act. Such an entity may remit, transmit, or deal in digital tokens that are not securities and because these tokens are not a recognized national currency of a foreign country and are not considered "funds" within the meaning of the PC Act, such activities alone do not yet bring the entity within the scope of acting as a money services business under the PC Act.

However, entities dealing in digital tokens that are not securities do not operate in a legislative vacuum across Canada. If an entity operates an automated teller machine or trading platform for digital tokens in Québec, the AMF has taken the position that such entities are money services businesses for the purposes of Québec legislation and must be licensed as such.[33]

V. COMMODITIES AND DERIVATIVES

Although the Bank of Canada has said that "digital currencies" are currently treated as commodities,[34] this has not been formally accepted or adopted by the CSA or other regulators. Some OSC staff have publicly complained that the Bank of Canada has not come out with a position as to whether bitcoin, ether, or any other coin is currency.[35]

In Canada, contracts for the sale of commodities, other than exchange-traded commodity futures contracts, could still qualify as investment contracts and thus be "securities" regulated by the provincial and territorial securities laws.

The CSA noted in CSAN 46-307 that digital tokens may also constitute derivatives and be subject to the derivatives laws adopted by the Canadian securities regulatory authorities;[36] however, the application of commodity trading laws and derivatives laws to digital tokens in Canada remains to be determined.

33 Autorité des marchés financiers, *Virtual currency ATMs and trading platforms must be authorized* (Montreal: Autorité des marchés financiers, 2015), online: https://lautorite.qc.ca/en/general-public/media-centre/news/fiche-dactualites/virtual-currency-atms-and-trading-platforms-must-be-authorized/.

34 Bank of Canada, *Briefing on Digital Currencies* (Ottawa: Senate of Canada, 2014), online: https://www.bankofcanada.ca/2014/04/briefing-on-digital-currencies/.

35 Alexandra Posadzki, "Bank of Canada has 'head in the sand' on Bitcoin: OSC", *The Globe and Mail* (30 October 2017), online: https://www.theglobeandmail.com/report-on-business/streetwise/bank-of-canada-has-head-in-the-sand-on-bitcoin-osc/article36772878/.

36 *Canadian Securities Administrators, supra* note 83.

VI. ENFORCEMENT PROCEEDINGS

Recent events suggest that caution must be exercised when considering the launch of, or the investment in, digital token distributions.

On July 20, 2017, the AMF obtained prohibition orders against various parties in connection with soliciting investments in PlexCoin, a digital token.[37] The PlexCoin "purported" ICO proceeded regardless in August. On December 8, 2017, the Québec Superior Court sentenced the individual behind PlexCoin to jail and fines for contempt of the court orders. On December 1, 2017, the United States Securities and Exchange Commission filed charges against the parties behind PlexCoin, describing the individual as "a recidivist Quebec securities law violator" and the ICO as a "full-fledged cyber scam."[38]

37 Autorité des marchés financiers, *Virtual Currency - Orders issued against PlexCorps, PlexCoin, DL Innov inc., Gestio inc. and Dominic Lacroix* (Montreal: Autorité des marchés financiers, 2017), online: https://lautorite.qc.ca/en/general-public/media-centre/news/fiche-dactualites/virtual-currency-orders-issued-against-plexcorps-plexcoin-dl-innov-inc-gestio-inc-and-dominic/.

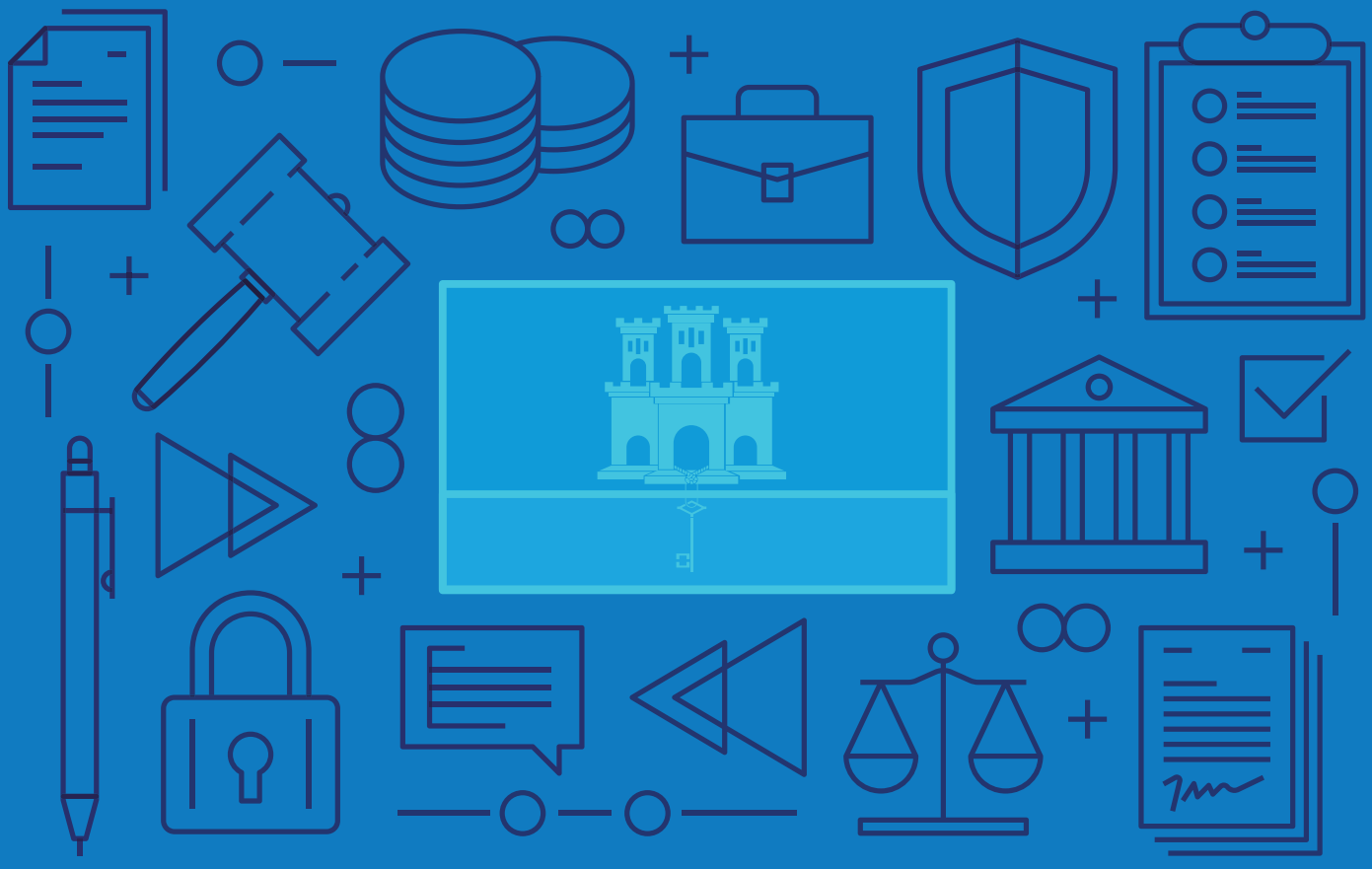
38 U.S. Securities and Exchange Commission, *SEC Emergency Action Halts ICO Scam* (Washington: U.S. Securities and Exchange Commission, 2017), online: https://www.sec.gov/news/press-release/2017-219.

TOKEN ALLIANCE

CHAMBER OF DIGITAL COMMERCE

UNDERSTANDING DIGITAL TOKENS

Legal Landscapes Governing Digital Tokens in Gibraltar



Prepared by the Token Alliance – an industry initiative of the Chamber of Digital Commerce

FIRST EDITION • JULY 2018

II. PART 1: REGULATORY OVERVIEW OF DIGITAL TOKEN MARKETS

SECTION 5: GIBRALTAR

I. INTRODUCTION

On 1st January 2018, Her Majesty's Government of Gibraltar ("HMGOG") brought into effect a new distributed ledger technology ("DLT") regulatory framework ("DLT Framework") defined on a principles basis with the ability to be applied proportionately to the business in question, providing businesses with the regulatory certainty that has been pursued by so many for so long. The intention is not to exclude certain activity from the existing regulatory framework but, rather, to build out a specific framework for businesses that use DLT to "store or transmit value belonging to others" by way of business, and that may not have been subject to regulation under another existing framework in Gibraltar. Similarly, the purpose is to build a framework that can continue to evolve and allow for the Gibraltar Financial Services Commission ("GFSC") to set appropriate and proportionate conditions or restrictions.

The DLT Framework includes nine principles applied to DLT firms operating in Gibraltar. The response to this approach has been global and truly significant with a large number of well-known businesses applying for licenses under the regulatory regime. Those who know nothing about Gibraltar may be surprised, but those who know the history of a small jurisdiction being 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.

In addition to the above, the GFSC released a public statement on 22nd September 2017 noting the increasing use of digital tokens based on DLT as a means of raising finance, especially by early stage start-ups. The GFSC also noted that these new ventures were highly speculative and risky, that early-

stage financing is often best undertaken by experienced investors, and set out matters that ought to be considered by anyone thinking of investing in digital tokens. In addition, the statement set out an intention to regulate the "promotion and sale of [digital] tokens."[1,2] HMGOG has publicly announced its intention to introduce regulations relating to, amongst other things, the promotion and sale of digital tokens in and from Gibraltar and set out its proposals in a document issued on 12th February 2018 (the "Token Framework Proposal").

II. THE GIBRALTAR REGULATORY FRAMEWORK

Digital tokens vary widely in design and purpose. In some cases, they may represent securities, such as shares in a company, and their generation and distribution are already covered by existing securities legislation in Gibraltar such as the Prospectuses Act 2005.[3] The 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 the Markets in Financial Instruments Directive (MiFID) II,[4] transposed into Gibraltar law through the Financial Services (Markets in Financial Instruments) Act 2018,[5] 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).

As a British Territory and current member of the European Union ("E.U."), the applicability of other existing frameworks would also need to be considered in the digital token context - electronic money issuance ("E-money") being an example. Even within the E.U., there are differing interpretations of the applicability of different regimes or rules. In the context of digital tokens, the tokens must represent a claim on the issuer in order to fall within the definition of "electronic money."[6] This might be the case for some digital tokens; however, utility tokens, as a rule, are usually not issued for the purpose of making payment transactions. This may not be the case for digital tokens that serve a cryptocurrency use; but even then, these tokens usually tend not to represent monetary value. It is characteristic for E-Money that it represents fiat and stores its value, backed by a claim on the token issuer for redemption against fiat. Conversely, digital tokens issued at par value against fiat and furnished with the promise of the token

1 Gibraltar Financial Services Commission, Statement on Initial Coin Offerings, http://www.fsc.gi/news/statement-on-initial-coin-offerings-250.
2 The terms used in this Section are exclusive to the enacted and proposed legislation of Gibraltar.
3 Prospectuses Act 2005, http://www.gibraltarlaws.gov.gi/articles/2005-46o.pdf.
4 Directive 2014/65/EU of 15 May 2014 on markets in financial instruments and amending Directive 2002/92/EC and Directive 2011/61/EU.
5 Financial Services (Markets in Financial Instruments) Act 2018, http://www.gibraltarlaws.gov.gi/articles/2006-32o.pdf.
6 Financial Services (Electronic Money) Regulations 2011, http://www.gibraltarlaws.gov.gi/articles/2011s167.pdf.

issuer to be redeemed in exchange for fiat, and therefore being accepted as means of payment by third parties, would qualify as E-Money.

Similarly, collective investment scheme ("CIS")[7] law such as the Financial Services (Collective Investment Schemes) Act 2011[8] is another relevant legal consideration. A collective investment scheme is described 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."[9] There can be many scenarios where digital tokens may not be defined as "securities" but may still be deemed to represent units in a collective investment scheme. In this case, a number of points would need to be considered, including the relevant exemptions and carve outs that may, under certain circumstances, also be relevant.

In addition to the above, the definition of an alternative investment fund ("AIF") under the Financial Services (Alternative Investment Fund Managers) Regulations 2013,[10] which transposes the E.U. Directive relating to alternative investment funds, needs to be considered. An AIF is deemed to be any collective investment undertaking that raises capital from a number of investors with a view to investing it in accordance with a defined investment policy for the benefit of those investors. If the arrangement is considered to form an AIF, or a token is deemed to represent a unit in an AIF, there are multiple considerations that become relevant, both in terms of the sale, promotion, and management of that scheme as well as the depositary arrangements for those units.

In many cases, digital tokens should not normally risk being a CIS. More often, however, digital tokens serve some cryptocurrency or functional use that is unregulated, such as the advance sale of products that entitle holders to access future networks or consume future services, or virtual currency, serving principally as a medium of exchange within an ecosystem (or marketplace) of consumers and service providers. However, entities issuing such types of digital tokens may still have to comply with classic consumer protection law,[11] depending on the design of the digital token.

A. GIBRALTAR CONTRACT LAW

The law of contract in Gibraltar is similar to the law in England and Wales. English common law applies in Gibraltar in accordance with the English Law (Application) Act 1962.[12] Unlike certain civil law jurisdictions, there is no general duty of disclosure in pre-contractual negotiations relating to digital token sales. Such a duty only exists when there are particular reasons for disclosure. These can be

7 Financial Services (Collective Investment Schemes) Act 2011, http://www.gibraltarlaws.gov.gi/articles/2005-48o.pdf; Financial Services (Collective Investment Schemes) Regulations 2011, http://www.gibraltarlaws.gov.gi/articles/2011s190.pdf; Financial Services (Alternative Investment Fund Managers) Regulations 2013, http://www.gibraltarlaws.gov.gi/articles/2013s103.pdf.
8 Financial Services (Collective Investment Schemes) Act 2011, http://www.gibraltarlaws.gov.gi/articles/2005-48o.pdf.
9 Financial Services (Collective Investment Schemes) Act 2011, http://www.gibraltarlaws.gov.gi/articles/2005-48o.pdf.
10 Financial Services (Alternative Investment Fund Managers) Regulations 2013, http://www.gibraltarlaws.gov.gi/articles/2013s103.pdf.
11 Consumer Protection (Unfair Trading) Act 2008, http://www.gibraltarlaws.gov.gi/articles/2008-18o.pdf; Financial Services (Distance Marketing) Act 2006, http://www.gibraltarlaws.gov.gi/articles/2006-23o.pdf.
12 English Law (Application) Act 1962, http://www.gibraltarlaws.gov.gi/articles/1962-17o.pdf.

based on a pre-existing relationship between the parties (*e.g.*, a fiduciary or confidential relationship)[13] or when the nature of the contract carries specific duties of disclosure (this can be the case in consumer contracts, where duties of disclosure are imposed by the relevant legislation – see below).

Participants in digital token issuances dealing with token issuers at arm's length are therefore expected to conduct due diligence. Unless one party's mistake of fact is due to misrepresentation by the other party (or some other vitiating factor, such as duress), the parties will usually be held to their contractual commitments under Gibraltar law.

In short, a token issuer in Gibraltar is under no general duty of pre-contractual disclosure, but is prevented from inducing a purchase of digital tokens by misrepresenting (whether fraudulently or negligently) the nature of the arrangement.

B. IMPLEMENTATION OF E-COMMERCE AND CONSUMER PROTECTION REGULATIONS INTO GIBRALTAR LAW

All relevant E.U. legislation covering e-commerce and consumer protection has been transposed into Gibraltar law via various Acts of Parliament or Regulations. The E.U. e-commerce and consumer protection rules (E-Commerce Directive,[14] Consumer Rights Directive,[15] Directive on Distance Marketing of Consumer Financial Services[16]) all specify the information that should be disclosed. The relevant provisions applicable under Gibraltar law are detailed below.

1. INFORMATION OBLIGATIONS WHEN GENERATING DIGITAL TOKENS VIA THE INTERNET

If the digital token is offered online, it falls within the scope of the E.U.'s e-commerce Directive, which has been transposed in Gibraltar through the Electronic Commerce Act 2001.[17] Regarding the type of information that must be provided when concluding electronic contracts, Section 6(1) states:

A service provider shall ensure (unless agreed otherwise with a prospective party to the contract who is not a consumer) that the following information is available clearly and in full before conclusion of the contract –

(a) the steps to follow to conclude the contract;

(b) whether the contract, when concluded, will be accessible and, if so, where;

13 Tate v. Williamson LR 2 Ch App 55 (1866).
14 Directive 2000/31/EC of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market.
15 Directive 2011/83/EC of 25 October 2011 on consumer rights.
16 Directive 2002/65/EC of 23 September 2002 concerning the distance marketing of consumer financial services.
17 Electronic Commerce Act 2001, http://www.gibraltarlaws.gov.gi/articles/2001-07o.pdf.

(c) the steps to follow to correct any errors made in input by the recipient of the service; further, such steps must be effective and accessible allowing the recipient to identify and correct any errors without difficulty;

(d) any general terms and conditions imposed by the service provider, further, such general terms and conditions must be accessible to the recipient of the service for him to store and retrieve them.[18]

2. DUTY TO PROVIDE INFORMATION UNDER CONSUMER PROTECTION LAW

If the contract on which a digital token is based constitutes a consumer contract, further consumer protection rules apply, as set out in the Consumer Rights on Contracts Regulations 2013[19] (which transposes, inter alia, the EU Consumer Rights Directive). These rules are highlighted under Part 2 of the Consumer Rights on Contracts Regulations 2013. The Regulations further split the specific information obligations in relation to off-premises and on-premises contracts under Schedule 1 and Schedule 2 respectively.

C. MONEY LAUNDERING

The E.U. Anti Money Laundering Directive has been transposed into Gibraltar law by the Proceeds of Crime Act ("POCA").[20] It should be noted that Section 9(1)(p) of the POCA now includes within the definition of "relevant financial business" that include "undertakings that receive, whether on their own account or on behalf of another person, proceeds in any form from the sale of tokenized digital assets involving the use of distributed ledger technology or a similar means of recording a digital representation of an asset."[21] POCA also requires reporting (by businesses and by the GFSC) when there is a suspicion (rather than actual knowledge) of money laundering. Essentially, the addition of the new definition of relevant financial business specifically brings sales of a tokenized digital asset clearly within existing AML laws, which in turn have been very well received by other service providers in the industry. Amongst other things, customer due diligence is required before a business may receive proceeds from the sale of tokenized digital assets. These businesses would also be required to appoint a money-laundering reporting officer (''MLRO''), as well as apply certain record keeping requirements. The business must also maintain an AML compliance program and report suspicious activity.

III. PROPOSED REGULATORY FRAMEWORK

As set out above, most often digital tokens do not qualify as securities under Gibraltar or E.U. legislation.[22] In the event that they do constitute securities, there is currently an E.U.-wide framework[23]

18 Electronic Commerce Act 2001, http://www.gibraltarlaws.gov.gi/articles/2001-07o.pdf.
19 Consumer Rights on Contracts Regulations 2013, http://www.gibraltarlaws.gov.gi/articles/2013s177.pdf.
20 Proceeds of Crime Act 2015, http://www.gibraltarlaws.gov.gi/articles/2015-22o.pdf.
21 Proceeds of Crime Act 2015, http://www.gibraltarlaws.gov.gi/articles/2015-22o.pdf.
22 HM Government of Gibraltar, Proposals for the regulation of token sales, secondary token market platforms, and investment services relating to tokens, http://gibraltarfinance.gi/20180309-token-regulation---policy-document-v2.1-final.pdf.
23 Prospectuses Act 2005, http://www.gibraltarlaws.gov.gi/articles/2005-46o.pdf.

dealing with this. Accordingly, Gibraltar is not looking to introduce a framework that will replace securities law or prospectus directive requirements. That is to say, the public offering of tokens that constitute securities do not require further regulation from a Gibraltar perspective and will continue to fall under current frameworks governing issuances of securities.

As of the date of writing, we do not know the full extent of HMGOG's legislative proposals for the regulation of digital token issuances, as the draft legislation has not yet been published. However, the Token Framework Proposal ("Framework")[24] provides a high-level outline of what lies in store. It is proposed that new legislation will regulate the following activities conducted in or from Gibraltar:

» The promotion and sale of digital tokens;

» The operation of secondary market platforms trading in digital tokens; and

» The provision of investment and ancillary services relating to digital tokens.

It is proposed the GFSC will regulate:

» Authorized sponsors of public digital token offerings;

» Secondary token market operators; and

» Digital token investment and ancillary service providers.

The Framework will not regulate:

» Technology;

» Digital tokens, smart contracts, or their functioning;

» Individual public offerings; or

» Persons involved in the promotion, sale, and distribution of digital tokens.

The following Sections set out at a high level the scope of the new proposed Framework.

A. DISCLOSURE RULES

The first limb of the Framework intends to deal with digital tokens that are not regarded as securities within the meaning of Gibraltar law. As set out above, this would typically cover circumstances where a digital token constitutes a product or service that does not yet exist (or is not substantially functional at the time of sale), in effect no more than a hope or ambition to deliver that product or service in the future. In such cases, purchasers risk that the product might never be delivered and often waive the right to the return on the price paid. HMGOG aims to ensure that whilst the purchaser

24 HM Government of Gibraltar, Proposals for the regulation of token sales, secondary token market platforms, and investment services relating to tokens, http://gibraltarfinance.gi/20180309-token-regulation---policy-document-v2.1-final.pdf.

may be prepared to take that risk, it is appropriate that they be presented with all the relevant information to enable them to make an informed decision. This limb of the Framework will therefore counter the current position in Gibraltar whereby a token issuer is under no general duty of pre-contractual disclosure.

With respect to the promotion, sale, and distribution of digital tokens, the Framework will require adequate, accurate, and balanced disclosure of information to enable anyone considering purchasing digital tokens to make an informed decision. The regulations may prescribe what, as a minimum, constitutes adequate disclosure, and in what form disclosures are made (*e.g.*, in a key facts document not exceeding two (2) pages). From time to time, guidance on disclosure rules may be published by GFSC.

The digital token industry often refers to the concept of "self-regulation," and best practice frameworks for token offerings have already been established. The key difference with the proposed regulations is that the concept of self-regulation, while being attractive in the sense that it may be said to decentralize certain standards and requirements, it is also in many senses 'voluntary' and does not necessarily raise the standards through any legally enforceable framework such as the one being proposed in Gibraltar. As a result, the GFSC can ensure and enforce their regulatory objectives through the implementation of the Framework.

B. FINANCIAL CRIME PROVISIONS

As discussed above, a recent amendment to POCA under Section 9(1)(p) means that token issuers now fall under its scope. It remains to be seen whether this amendment is a temporary measure which will be replaced by specific regulations on AML and CFT once the Framework comes into force or whether these amendments were in fact what was contemplated in the Framework. Nevertheless, this demonstrates the intention of the Gibraltar Government to ensure that, even before the proposed digital token regulations come into force, existing statutory safeguards require all token issuers to carry out due diligence on digital token purchasers and to mitigate AML/CFT risks.

C. AUTHORIZED TOKEN SPONSORS

As outlined above, the GFSC intends to regulate:

- Authorized sponsors of public token offerings;
- Secondary token market operators; and
- Digital token investment and ancillary service providers.

It therefore appears that the onus of ensuring compliance with appropriate standards will be on the service providers and secondary token market operators and the GFSC does not intend to regulate token issuers, nor will it regulate the underlying technology or the digital tokens themselves.

The Framework will establish a regime for the authorization and supervision of token sponsors possessing appropriate relevant knowledge and experience who will be responsible for compliance with this limb of the regulations. It is intended that an authorized token sponsor will need to be appointed in respect of every public token offering promoted, sold or distributed in or from Gibraltar.

Token sponsors will be subject to an authorization and supervision process by the GFSC and must possess suitable knowledge and experience of the industry to be admitted into the sponsorship regime. A critical component for token sponsors to be authorized is to have local presence in Gibraltar, with "mind and management" based in the jurisdiction. The onus will also be on token sponsors to produce their own codes of conduct, setting out what they consider to be best practices relating to token offerings. These codes will form part of a prospective token sponsor's application for authorization. The introduction of a token sponsor regime is comparable to what currently exists today in the U.K. in relation to regulated public market listings, where Sponsors and Nominated Advisors effectively act as listing agents that guide prospective issuers through the flotation process. It appears this same model is being adapted under the token sponsor regime to handhold prospective token issuing entities through a compliant token sale process.

The GFSC will establish and maintain a public register of authorized sponsors and their respective past and present codes of practice.

D. SECONDARY MARKET OPERATIONS

Apart from the DLT Framework, operating a secondary market platform for trading tokens is not currently regulated in Gibraltar. The Framework will regulate the conduct of secondary market platforms, operated in or from Gibraltar and, to the extent not covered by other regulations, their derivatives, with the aim to ensure that such markets are fair, transparent, and efficient.

At this stage, the Framework does not elaborate on the specific regulatory obligations that will be imposed. However, it does highlight the introduction of further transaction reporting and disclosure requirements, as well as extending the application of the Framework to cover trading of derivative token products. The Framework does, however, mention modeling the proposed regulations on market platform provisions under MiFID II[25] and the Markets in Financial Instruments Regulation (MiFIR),[26] so far as is appropriate, proportionate, and relevant.

E. INVESTMENT AND ANCILLARY SERVICE PROVIDERS

Providing investment and ancillary services relating to digital tokens is not currently regulated in Gibraltar. HMGOG has proposed to regulate the provision of investment and ancillary services in or from Gibraltar and, to the extent not otherwise caught by regulations, their derivatives. These

25 Directive 2014/65/EU of 15 May 2014 on markets in financial instruments and amending Directive 2002/92/EC and Directive 2011/61/EU.
26 Regulation (EU) No 600/2014 of 15 May 2014 on markets in financial instruments and amending Regulation (EU) No 648/2012.

regulations aim to ensure that such services are provided fairly, transparently, and professionally. This limb of the Framework will intend to cover advice on investment in digital tokens, virtual currencies, and central bank-issued digital currencies, including:

- generic advice (setting out fairly and in a neutral manner the facts relating to token investments and services);
- product-related advice (setting out in a selective and judgmental manner the advantages and disadvantages of a particular token investment and service); and
- personal recommendations (based on the particular needs and circumstances of the individual investor).

This limb of the Framework will be proportionately modeled on provisions that currently exist under MiFID II[27] with the aim of ensuring that such services are provided fairly, transparently, and professionally. However, at this stage, little guidance has been given on the specific types of advisors involved in a digital token distribution process that will be caught by the proposals (*e.g.*, introducers, marketing professionals, technical developers and smart contract auditors, economic, legal and tax advisors, cybersecurity firms, escrow agents, etc.).

IV. DLT SERVICES

As set out above, the DLT Framework is a licensing regime for individuals and firms that engage in activities that, for business purposes, use DLT for the transmission or storage of customers' assets. It is generally accepted that the DLT Framework does not extend to the generation and sale of digital tokens. This is in line with public statements made by various bodies, including HMGOG, and is consistent with the Framework which will be introduced for these purposes. However, there may be instances where a token issuer may fall within the scope of the DLT Framework, although this should be considered separately from the actual digital token sale, which may remain unregulated until the new legislation referred to above comes into effect.

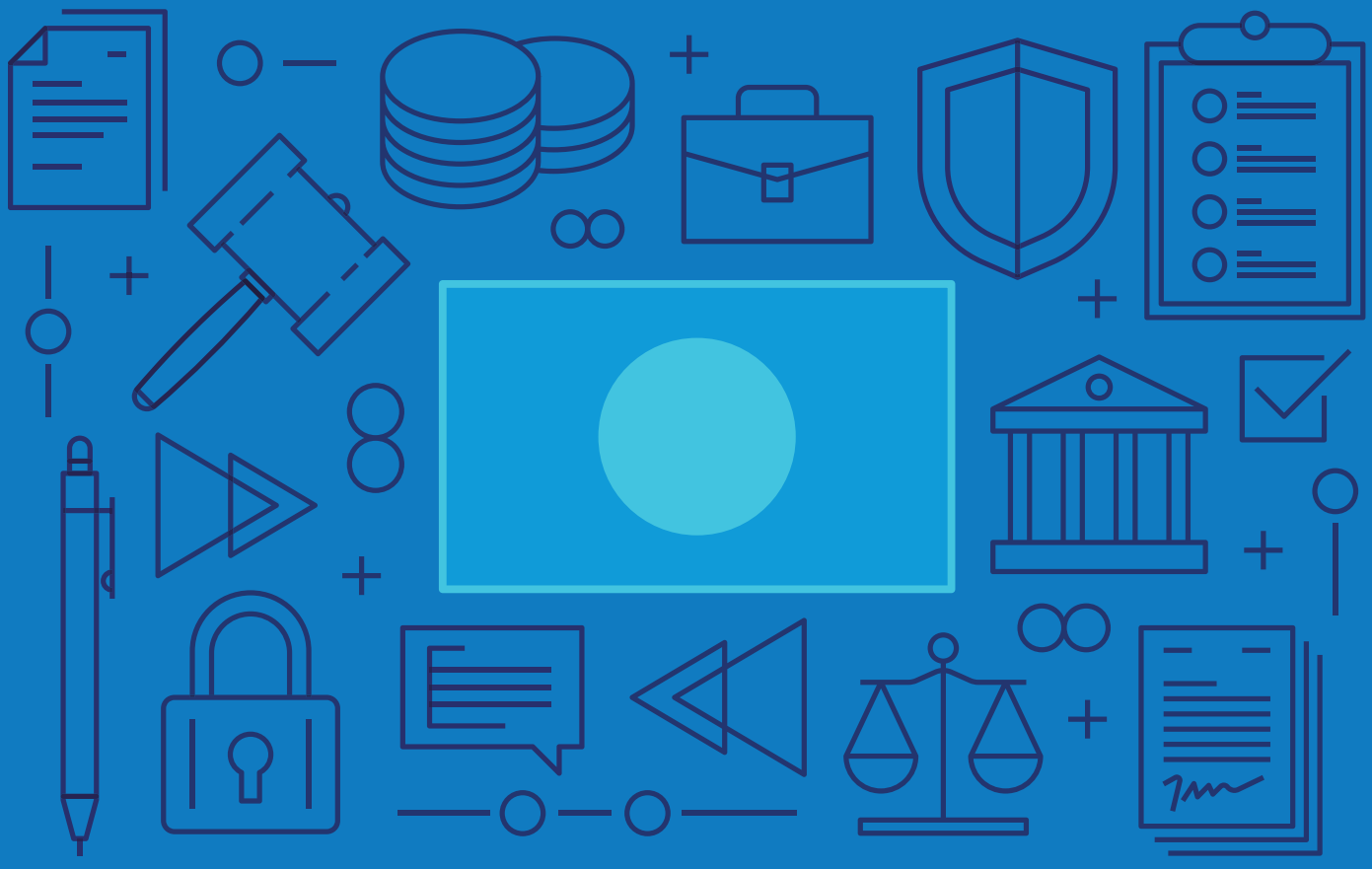
27 Directive 2014/65/EU of 15 May 2014 on markets in financial instruments and amending Directive 2002/92/EC and Directive 2011/61/EU.

TOKEN ALLIANCE

CHAMBER OF DIGITAL COMMERCE

UNDERSTANDING DIGITAL TOKENS

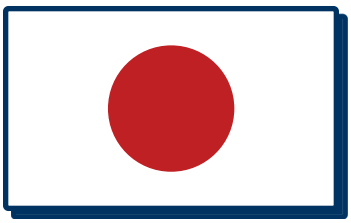
Legal Landscapes Governing Digital Tokens in Japan



Prepared by the Token Alliance – an industry initiative of the Chamber of Digital Commerce

FIRST EDITION • SEPTEMBER 2019

TABLE OF CONTENTS



I. INTRODUCTION

Although the concept of digital tokens does not exist under Japanese law, the concept of "virtual currency", a subset of digital tokens, does.[1] While virtual currency is a concept different from fiat currencies and securities, as detailed below, almost all of the digital tokens that are not denominated in fiat currency are deemed to be virtual currency. Therefore, when contemplating a business involving digital token transactions, it is necessary to consider regulations governing virtual currency.

Several laws in Japan comprise the regulatory framework around virtual currency. The Payment Services Act (the "PSA")[2] is the primary law within the framework; however, the Financial Instruments and Exchange Acts (the "FIEA"); the Act Regulating the Receipt of Contributions, Receipt of Deposits and Interest Rates; and the Money Lending Business Act (among others) should also be examined when determining whether to engage in business activity related to virtual currency. These laws are enforced by the Japanese Financial Services Agency (the "JFSA"), which supervises the virtual currency industry and works with the Japanese Virtual Currency Exchange Association (the "JVCEA"), the industry's self-regulatory organization.

Following the hack of Mt. Gox, a virtual currency exchange that was headquartered in Japan, and the Financial Action Task Force's ("FATF") guidance in 2015,[3] recommending that "virtual currency exchange service providers" be registered or licensed and subject to AML standards substantially similar to that of other financial institutions, prompted Japan to take regulatory action swiftly. Hence, amendments to the PSA and the Act on Prevention of Transfer of Criminal Proceeds (the "AML Law")[4] came into effect as of April 1, 2017 (the "Effective Date"). The PSA, as amended, included stipulations for the terms "virtual currency", "virtual currency exchange service", and "virtual currency exchange service provider".

Where the relevant digital token is deemed virtual currency under the PSA, depending on the manner in which such virtual currency is transacted, the regulation imposed on virtual currency exchange service providers needs to be examined. For example, amendments to the AML Law in 2017 subject virtual

1 In December 2018, the Japanese government proposed to replace the term "virtual currency" with "crypto asset". The laws, however, have not yet been updated to reflect the proposed change.
2 Act No. 59 of June 24, 2009, http://www.japaneselawtranslation.go.jp/law/detail/?id=3078&vm=02&re=02.
3 FATF, Guidance for a Risk-Based Approach to Virtual Currencies, http://www.fatf-gafi.org/publications/fatfgeneral/documents/guidance-rba-virtual-currencies.html.
4 Act No. 22 of March 31, 2007.

currency exchange service providers to the regulations for anti-money laundering and counter-terrorism financing ("AML/CTF").

Where quasi-financial instruments are transacted concerning digital tokens, there may be a case where the regulations pursuant to the FIEA[5] should be investigated. While digital tokens will not fall under financial instruments, in principle, they may nonetheless be regulated by the FIEA under certain circumstances, such as if tokens are issued in an attempt to circumvent the FIEA or in an initial coin offering ("ICO") scheme entailing dividends.

Depending on the form of the transaction, applicability of other laws, such as the Act Regulating the Receipt of Contributions, Receipt of Deposits and Interest Rates[6] and the Money Lending Business Act may well be considered.[7]

The JFSA imminently contemplates reforming crypto asset regulations to address the problems that arose after Phase 1 of the virtual currency legislation which became effective in April 2017. The JFSA published a draft bill for the amendments to the PSA and the FIEA on March 15, 2019. The discussion in Sections II and III below is based on the current state of laws. For the outline of the amendments proposed in the bill, please refer to Section IV below.

Following two massive virtual currency hacking incidents, the JFSA tightened its oversight of virtual currency exchange service providers, including imposing stricter registration requirements and on-site inspections. It issued a number of business improvement orders and suspended a few virtual currency exchange service providers.

In light of highly volatile virtual currency prices and explosive trading volumes in 2017, a surge of ICOs in 2017, and hacking incidents in 2018, the JFSA created the Study Group on Virtual Currency Exchange Services[8] in March 2018 to discuss appropriate crypto asset regulations. After eleven (11) sessions of discussion, the group published a final report in December 2018.[9] The JFSA drafted bills based on this report and the national government submitted the draft to the Diet, Japan's legislative body, on March 15, 2019. The discussion below focuses on the current laws and then compares it with the proposed laws.

The timeline for enactment remains uncertain. The national government submitted the amended bill to the Diet on March 15, 2019, and the Diet will discuss them. The following timeline is anticipated:

1. The Diet will approve the bill in May.

2. The JFSA will draft government ordinances and guidelines which are subordinated rules of the

5 Act No. 25 of April 13, 1948; Financial Instruments and Exchange Act, http://www.japaneselawtranslation.go.jp/law/detail/?ft=2&re=02&dn=1&yo=financial&x=0&y=0&ia=03&ph=&ky=&page=16.
6 Act No. 195 of June 23, 1954.
7 Act No. 32 of May 13, 1983.
8 Publication of Report from Study Group on Virtual Currency Exchange Services, https://www.fsa.go.jp/en/refer/councils/virtual-currency/20181228.html.
9 Report from Study Group on Virtual Currency Exchange Services, https://www.fsa.go.jp/en/refer/councils/virtual-currency/20181221-1.pdf.

amended laws and the drafts will be released for public review and comment around October to December 2019. The comprehensive list of the final public comment hearing results on the 2019 proposed government ordinances and guidelines and the final form thereof will be released around the end of 2019 to March 2020.

3. The amended law will be valid within one year after the enactment of the acts expected in around April or May 2020.

4. Some of the new regulations, such as regulation on custody and derivatives, have a six-month (6) transition period after enactment.

II. REGULATION OF VIRTUAL CURRENCY AS DEFINED UNDER THE PAYMENT SERVICES ACT

When contemplating a business involving digital token transactions, it is important to determine first, if it is a virtual currency and, second, if such business is deemed a virtual currency exchange service.

A. VIRTUAL CURRENCY

Under the PSA, virtual currencies are classified as either Type I or Type II virtual currencies based on their function:[10]

> **Type I Virtual Currency:** property value (limited to that which is recorded on an electronic device or any other object by electronic means, and excluding the Japanese currency, foreign currencies, and currency-denominated assets; the same applies to the following item) which can be used in relation to unspecified persons for the purpose of paying consideration for the purchase or leasing of goods or the receipt of provision of services and can also be purchased from and sold to unspecified persons acting as counterparties, and which can be transferred by means of an electronic data processing system.
>
> **Type II Virtual Currency:** property value that can be mutually exchanged with what is set forth in the preceding item with unspecified persons acting as counterparties, and which can be transferred by means of an electronic data processing system.

In short, digital tokens that can be used for the purpose of paying and can also be purchased from and sold to unspecified persons acting as counterparties are Type I virtual currency, such as bitcoin, litecoin, ether, and other virtual currencies that can be used as a payment method. Digital tokens that can be mutually exchanged with Type I virtual currency are Type II virtual currencies. Tokens that are linked to any fiat currency are regulated by another provision in the PSA.

In this regard, the JFSA currently deems almost all digital tokens (*e.g.*, alt-coins, ICO tokens, and so on) to be virtual currency, except for fiat currency-denominated assets (*e.g.*, Suica, a fiat-denominated

10 Paragraph (5) Article 2, PSA.

prepaid e-money card). The JFSA broadly construes the elements of virtual currency such that it "can be used …for …paying", it "can also be purchased", and "can be mutually exchanged with" Type I virtual currency; *i.e.*, digital tokens may be deemed Type I virtual currency (or Type II virtual currency, as the case may be,) so long as they have a possibility in the future to be used, purchased, and exchanged.[11]

B. VIRTUAL CURRENCY EXCHANGE SERVICES

Under the PSA, virtual currency exchange services are subject to registration requirements, various code of conduct rules, and supervision.

The term "virtual currency exchange service" means any of the following acts that are carried out on a regular basis[12]:

i. Purchase and sale of a virtual currency (*i.e.*, exchange between a virtual currency and a fiat currency) or exchange with another virtual currency;

ii. An intermediary, brokerage, or agency service for the acts described above and;

iii. Management (custody) of a fiat currency or virtual currency on behalf of the users/recipients in relation to the acts described above in (i) or (ii).

Examples of businesses that might be deemed as conducting a virtual currency exchange service are:

- Exchanges in which users can sell and/or purchase virtual currency from other users;
- Shops that purchase and/or sell virtual currency;
- Bitcoin ATM operators;
- ICO issuers; and
- Brokerage firms that intermediate purchases or sales of virtual currency

Examples of businesses that do not fall under the definition of "virtual currency exchange services" are:

- Persons who trade virtual currency for their own investment purposes
- Mining firms
- Software developers

Currently, the PSA regulates virtual currency exchange businesses but excludes from regulation businesses that only offer custody services. The definition of a virtual currency exchange business

11 The term "virtual currency" appears solely in the PSA and the AML Law but in no other statutes.
12 Paragraph (7) Article 2, PSA.

above does not include custodial operations unrelated to the purchase and/ or sale of virtual currency (*e.g.*, a wallet service provider who does not engage in the purchase or sale of a virtual currency).

C. OBLIGATIONS OF VIRTUAL CURRENCY EXCHANGE SERVICE PROVIDERS

Virtual currency exchange service providers are obliged to register with the relevant local finance bureau (sub-division of the JFSA) that is authorized by the Prime Minister. As of March 27, 2019, nineteen (19) companies are registered with the JFSA to perform virtual currency exchange services.[13]

Virtual currency exchange service providers are under the following duties, amongst others, pursuant to the PSA:

- Establishment and maintenance of a business management system
- Compliance with the laws and regulations
- Customer identity verification at the time of transaction
- Measures for user protection
- Elimination of relationships with anti-social forces
- Management of users' assets (segregated management of funds or virtual currency deposited by the users)
- Management of information regarding the users
- Complaints management, financial ADR system, management of system risk
- Management of outsources and vendors
- Preparation and preservation of books and documents concerning virtual currency exchange service
- Submission of reports concerning virtual currency exchange service

Further, registered virtual currency exchange service providers are committed to abiding by the self-regulation rules drawn up by the JVCEA, Japan's virtual currency self-regulatory organization, which was established on April 23, 2018 by sixteen (16) registered virtual currency exchange service providers.[14] On October 24, 2018, the JVCEA was certified by the JFSA as a Certified Association for Payment Service Providers under the PSA.[15] The JVCEA established self-regulation rules in furtherance of the existing regulations that are based on, amongst others, the PSA, the AML Law, and the

13 The companies are: bitFlyer, Tech Bureau, QUOINE, bitbank, DMM Bitcoin, GMO Coin, SBI Virtual Currencies, BTC BOX, BIT Point, FISCO Cryptocurrency Exchange, Money Partners, Bit Ocean, Xtheta, Huobi Japan, TaoTao, Bitgate, Coincheck, Rakuten Wallet, DeCurret. List of Companies Registered with the JFSA, https://www.fsa.go.jp/menkyo/menkyoj/kasoutuka.pdf.

14 Japanese Virtual Currency Exchange Association, https://jvcea.or.jp.

15 About Authorization of Authorized Fund Settlement Business Association, https://www.fsa.go.jp/news/30/virtual_currency/20181024-1.html.

Guidelines for Administrative Processes concerning virtual currency exchange service providers ("FSA Guidelines") with a view to better protect users in light of the current service practice (such rules are roughly itemized below).

Items of self-regulation:

- Handling of virtual currency
- User property management
- Management of system-risk and information security
- Contingency
- AML/CFT
- Complaint processing and dispute processing
- Solicitation and advertisement
- User management
- Order management system
- Prevention of illicit transactions
- Management system of virtual currency related information
- Financial management

The self-regulation rules were drawn up with reference to the self-regulation rules pursuant to the FIEA concerning financial instruments exchange business (defined therein) implemented by the Japan Securities Dealers Association, a self-regulatory organization within the securities industry.

D. THE STATUS QUO OF REGISTRATION SCREENING

The JFSA's review process for granting registrations was tightened after the NEM-equivalent of approximately fifty-eight (58) billion yen was hacked from Coincheck, a virtual currency service provider, in January 2018. As a result, the JFSA did not approve any new virtual currency service providers to offer their services from when the incident occurred until January 11, 2019, when it approved Coincheck's application to offer virtual currency services. Two other applicants, Rakuten Wallet and DeCurret, subsequently became registered as virtual currency exchange service providers on March 25, 2019.

On February 1, 2018, all registered virtual currency exchange service providers and deemed registered virtual currency exchange service providers[16] were ordered to report on system risks. On-site inspections were first conducted on Coincheck and then on each registered and deemed registered virtual currency exchange service provider. Business improvement orders, business suspension orders, and refusals of registration were issued to the majority of the registered virtual currency exchange service providers and deemed registered virtual currency exchange service providers.

The JFSA reviewed registration screenings and monitoring processes, taking account of the reality and issues found in inspections. As a result, the requisite level for virtual currency exchange service providers to attain for successful registration (*e.g.*, internal control system, governance structure, system for system risk management, etc.) became at least as high as that of financial institutions, therefore significantly higher than that intended to be required when the PSA, as amended, was implemented.

Implementation of the said self-regulation rules has also effectively raised the bar for registration.

However, the JFSA did not cease to register new virtual currency exchange service providers. The JFSA continues to review new registration applications, and multiple applicants are expected in the near future to be registered as virtual currency exchange service providers.

E. PROPOSED AMENDMENTS TO THE PSA

The Diet will review the following proposals to amend the PSA: 1) the term "virtual currency" will be altered to "crypto assets" in the amendments to the PSA; and 2) additional duties will be imposed on crypto asset exchange services.

Crypto assets exchange service providers will be subject to the following requirements in addition to the requirements that are currently imposed. Amongst the newly-added requirements are:

- To manage crypto assets in cold wallets. Certain crypto assets that satisfy prescribed conditions may be managed in a hot wallet.
- To hold and reserve proprietary crypto assets of the same kind and of the same value as the customer's crypto assets managed in a hot wallet.
- To prohibit advertisement and solicitations to indicate false or misleading information or to induce speculative trading.
- To make prior notification to the JFSA of any change in tradable crypto assets or scope of crypto assets exchange service.

16 The PSA avails certain interim measures for those early market entrants that started their Virtual Currency Exchange Business no later than 31 March 2017 (before the effective date of the amendments to the PSA to stipulate Virtual Currency Exchange Service). To the extent such business operator applied for registration, and such application was officially received by JFSA on or before 30 September 2017, it is permitted to continue as a Virtual Currency Exchange Business until registration is granted or refused.

Clearly, one of the most onerous burdens would be the second item. The definitions of "hot wallet" and "cold wallet" are not stipulated in the draft law, and we believe that the JVCEA will take this up.

Moreover, under the amended PSA, in the event of insolvency of a crypto asset exchange service provider, customers will be vested with the right to receive payment in preference to other creditors. Meanwhile, the amended FIEA will regulate unfair trading — not only crypto asset exchange service providers but every person, including customers. Unfair trading includes engaging in fraudulent or deceptive acts, intimidation, and market manipulation; it does not include insider trading, which is not specifically prohibited.

The prohibition of unfair trading includes engaging in fraudulent acts, following but does not include prohibition of insider trading:

- Prohibition of unfair trading
- Prohibition of fraudulent acts, spreading rumors, using fraudulent means or intimidation
- Prohibition of market manipulation.

As set out in the discussion around virtual currency exchange services, the PSA regulates virtual currency exchange businesses but not standalone custody service providers. The amended PSA will regulate such custody service. The definition of custody is "to manage crypto assets for others except for the case such business is allowed in other laws." Such custodial service providers will not be able to provide service to Japanese residents without a license.

As the definition of "custody service" is unclear, the types of custody businesses that will be regulated are still uncertain. Generally speaking, we believe that businesses that hold customers' private keys and send/transfer crypto assets for customers will be regulated.

Amongst the regulations on crypto asset exchange service providers, the regulations on the management of the crypto assets (*e.g.*, duty of customer identification/ KYC, segregated management of customers' assets) would be applied to crypto asset custodial services, with the details thereof awaiting the cabinet office order on crypto assets exchange service providers to come.

III. REGULATIONS FOR ICOS

An ICO is a form of fundraising by selling so-called "coins" or "tokens". The ICO remains a global topic that is being followed with untiring enthusiasm. Whereas, it was pointed out that such ICOs originated as breakthroughs to allow retail investment, some ran counter to user protection principles (*e.g.*, the rights represented by the tokens were obscure, the business plan was lax/sloppy, or the scheme itself was fraudulent).

On October 27, 2017, the JFSA publicized its view in the paper "Initial Coin Offerings ("ICOs") — users and service providers warning about the risks of ICOs".[17] The JFSA alerted users and service providers of the risks of an ICO, specifically referring to the possible applications of the PSA and the FIEA as triggered by the structure of the token offering. The JFSA, seemingly, deems most ICO schemes to be subject to the regulations by the PSA and requires registration of the ICO issuer/platformer as a virtual currency exchange service provider. For the purpose of registration as an ICO issuer, the requisite level is still under discussion and remains to be defined by the JFSA. Consequently, ICOs that have launched after December 2017, when the JFSA began reviewing the registration process for ICOs, have done so without registering with the JFSA and may not be in compliance with the laws since registration is required.

A. THE REQUIREMENT TO REGISTER A VIRTUAL CURRENCY EXCHANGE SERVICE FOR ICOS

In order to conduct an ICO, even where the ICO tokens issued do not serve as a means of settlement or exchange facing unspecified persons, registration as a virtual currency exchange service and notification of the use of ICO tokens to the JFSA are required. The JFSA broadly construes the elements "can be used … for … paying", "can also be purchased", and "can be mutually exchanged with", *i.e.*, digital tokens may be deemed as Type I virtual currency (or Type II virtual currency, as the case may be) for so long as such coins have a possibility in the future to be used, purchased, and exchanged. By such interpretation by the JFSA, any ICO tokens may theoretically be used for settlement, sold or exchanged, etc.; thus, ICO tokens generally are deemed virtual currency.

Raising funds in fiat currency or in other virtual currency (such as bitcoin or ether) in exchange for an issuance of ICO tokens would constitute a virtual currency exchange service as in the definition of purchase and sale of a virtual currency (*i.e.*, exchange between a virtual currency and a fiat currency) or exchange with another virtual currency.

B. THE POSSIBILITY OF BEING SUBJECT TO FUND REGULATIONS

As detailed above, some ICO tokens meet the definition of securities as well as the definition of virtual currency. Thus, amongst the statutorily defined items of securities, the term "collective investment schemes (fund)" is a broad and diverse concept. Certain ICOs may fall under such collective investment schemes, specifically where an ICO is intended (i) to collect fiat money from others, (ii) to invest in a business, and (iii) to pay dividends to holders.

C. REGULATIONS FOR ICOS TO BE LAUNCHED IN JAPAN

The regulations delineated above will apply indiscriminately to the ICOs carried out by foreign service providers so long as any Japanese resident is targeted or solicited for a subscription of tokens.

17 Initial Coin Offerings – User and Business Operator Warning About the Risks of ICOs, https://www.fsa.go.jp/policy/virtual_currency/07.pdf.

In the event that any non-Japanese residents conduct an ICO while disregarding these regulations, the JFSA will alert such non-resident providers of the applicable Japanese regulations.

Currently, those wishing to solicit Japanese residents for subscriptions of ICO tokens must choose from the following two options while taking care to avoid inadvertently triggering the application of the fund regulations indicated above. The first such choice is to register as a virtual currency exchange service provider and sell tokens directly. The second is to delegate the sale of ICO tokens to a third party that is a registered virtual currency exchange service provider.

At the time of writing, no virtual currency exchange has been registered for the purpose of conducting an ICO, and from December 2017 onwards, no ICO has been launched as unequivocally in compliance with the laws. Still, ICO regulations are actively being discussed by the JFSA and JVCEA; thus, it is possible that Japan may be speedily equipped to host clear-cut legal ICOs in the near future. For the time being, however, since the timeframe for the registration process and the focal items examined in screenings remain obscure, it is virtually impossible to carry out an ICO in Japan under current law.

IV. THE FINANCIAL INSTRUMENTS EXCHANGE ACT

A. COMMON VIRTUAL CURRENCIES SUCH AS BITCOIN AND ETHER DO NOT FALL UNDER THE DEFINITION OF SECURITIES

The FIEA regulates financial instruments/securities/derivatives by exhaustively stipulating and defining them. For the FIEA to apply, the case must involve either "Negotiable Instruments/Securities" or "Derivatives" as defined therein. Common virtual currencies such as bitcoin and ether are not included in either "Negotiable Instruments/Securities" or "Derivatives." Hence, as a general rule, the Act does not apply to the sale and purchase or exchange of virtual currency.

B. COLLECTIVE INVESTMENT SCHEMES ARE REGULATED BY THE FIEA

A recent trend that we have seen in global markets, including in Japan, is that more funds are formed in virtual currency. Among ICO tokens, we observe tokens such as the ones designed to represent rights to the distribution of profit derived from the business carried out, as financed by the proceeds of the token sale. Based on these trends, these funds and ICOs may constitute a collective investment scheme under the FIEA. Hence, the current investment fund regulations likely do not apply to those funds raised in virtual currency or via ICO when raising virtual currency but not fiat currency.

Essentially, the FIEA defines a "collective investment scheme" as a structure that has the following three elements, irrespective of its legal form:

i. receipt of money (including those specified by the Cabinet Order as similar thereto, hereinafter referred to as "money, etc.") or contributions from other persons;

ii. such money is used to do business/projects; then,

iii. to distribute dividends of profits arising from such projects or distribute the assets of said business to investors or contributors of the said money.

To conduct a public offering or private placement of collective investment schemes in Japan generally, a fund must register as a Type II Financial Instruments Exchange Business be subject to the FIEA fund regulations.

To be clear, when tokens are offered in exchange for payment in virtual currency, such as bitcoin or ether, the FIEA Fund Regulations are unlikely to come into play since bitcoin and ether are not "money, etc." under Japanese law. However, if someone sells bitcoin or ether in exchange for cash to investors and then collects such bitcoin and ether from the investors as an investment to a fund, the chain of actions as a whole may be deemed to constitute collecting "money, etc." and, thus, may be regulated. Further, where such FIEA regulated funds are tokenized to be freely transferable, only the Private Trading System/PTS licensed operators pursuant to the FIEA may provide a secondary market for such tokens. Some believe that the quasi-financial instruments that are contributed not in "money, etc." but in virtual currency should likewise be regulated by the FIEA. Such views are discussed in a report published by the JFSA Study Group on Virtual Currency Exchange Services (April 2018–).[18] A prospective reform of the laws in this regard would deserve continued attention.

C. PROPOSED AMENDMENTS TO THE FIEA

1. REGULATIONS ON STOS

Tokens that grant their owners the rights to receive dividend of profits (Securities Token Offerings or "STO") are defined in the amended FIEA as the "property rights indicated and transferred electronically (PRITE)". PRITEs fall under a type of financial instruments identified in the FIEA as Paragraph 1 Securities[19] and are subject to the provisions of the amended FIEA. PRITEs are excluded from the definitions of the amended PSA as currently proposed.

In the amendments to the FIEA, STOs as categorized under Paragraph 1 Securities will be subject to the requirements for Disclosure of Corporate Affairs and Other Related Matters in the same manner that shares are subject thereto. The person engaged regularly in the purchase and/or sale with respect to STOs and intermediary or brokerage thereof must register itself as a Type I Financial Instrument Operator. If an issuer sells STOs by himself, he must register as a Type II Financial Instrument Operator, which is less complicated than Type I.

18 Publication of Report from Study Group on Virtual Currency Exchange Services, https://www.fsa.go.jp/en/refer/councils/virtual-currency/20181228.html.
19 Paragraph (3) Article 2, FIEA. Most typical examples of the Paragraph 1 Securities are shares and bonds.

As for the regulation of ICOs other than STOs, no major changes are being made by the legislative reform at this time. To conduct/carry out ICOs, it is believed that the registration of crypto assets exchange service providers and the filing of the coins/tokens with the JFSA will be required.

2. CRYPTO ASSETS DERIVATIVE TRANSACTIONS

Under the current FIEA, no specific provisions are set out in respect of the derivatives transactions with crypto assets as underlying assets. In the proposed amendments, the crypto assets are included in the definitions of financial instruments and crypto assets or financial indicators derivatives will be subject to the regulatory provisions in the FIEA in the same manner the FX transactions are currently subject thereto. Therefore, registration of Type I financial instrument exchange businesses will be required for the businesses to regularly engage in derivative transactions pertaining to crypto assets.

3. FUND REGULATIONS

As was stated in the discussion of obligations of virtual currency exchange service providers, provisions of the current FIEA would not apply to any fund (collective investment scheme) to which contribution is made in a virtual currency. In the proposed amendments to the FIEA, the crypto assets contributed by those who have the right to receive dividend of profits are deemed money. Therefore, the regulatory provisions in the FIEA will apply to funds contributed in crypto assets as consideration.

V. OTHER NOTABLE REGULATIONS

A. AML LAW REGULATIONS

The purpose of the AML Law is to prevent money laundering and the transfer of criminal proceeds and to ensure the appropriate enforcement of international treaties concerning the prevention of terrorist financing. The AML Law imposes such duties as listed below on certain specified business operators, including, but not limited to, financial institutions:

- Verification at the time of transaction of customer identification data (*e.g.*, name, domicile, and date of birth).
- Preparation and preservation of verification records.
- Preparation and preservation of transaction records and other documents concerning prescribed transactions.
- Reporting of suspicious transactions (*e.g.*, the proceeds of the transaction are suspected to be illicit) to the administrative agency with jurisdiction over the relevant specified business operator.

The AML Law now includes within its scope virtual currency exchange services. As a result, virtual currency exchange service providers are subject to the duties described above.

B. THE ACT REGULATING THE RECEIPT OF CONTRIBUTIONS, RECEIPT OF DEPOSITS, AND INTEREST RATES

When raising funds by way of ICO or virtual currency, care should be taken lest the fundraising inadvertently interfere with the Act that regulates the receipt of contributions, receipt of deposits, and interest rates (the Receipt of Contributions Act).

The Receipt of Contributions Act sets out provisions for, amongst others, restrictions on the receipt of contributions, the prohibition of receipt of deposits, punishment on usury, etc., but is all about transactions of money. Since virtual currencies do not, at least presently, qualify as money, an act of receiving deposits in virtual currencies is excluded from the regulations under the Receipt of Contributions Act.

On the other hand, raising fiat money by way of selling ICO tokens or virtual currency with a promise to refund the entire amount of the contribution or money equivalent to an amount exceeding the contribution as reimbursement at a later date might be deemed as such prohibited receipt of deposits under the Receipt of Contributions Act. When making a judgment if the Receipt of Contributions Act applies to any given transaction, consider first specifically and concretely the substance of such transaction such as a scheme but not whether the transaction technically is to receive contributions in virtual currency.

C. THE MONEY LENDING BUSINESS ACT

Where virtual currency is being lent as a business or on a regular basis, such business of lending virtual currency would not constitute “money lending” under the Money Lending Business Act by the fact that virtual currency may not be deemed as money.

Where a virtual currency exchange service offers advances or money lending to users through offering margin trading or leverage trade, pursuant to the Money Lending Business Act, the service provider shall be registered by the relevant local finance bureau that is authorized by the Prime Minister.

Making a loan in virtual currency currently does not constitute any act obliged to be registered as a virtual currency exchange service.

D. FOREIGN EXCHANGE AND FOREIGN TRADE ACT

Under the Foreign Exchange and Foreign Trade Act, (i) when a resident or a non-resident has received a payment made from Japan to a foreign state or a payment made from a foreign state to Japan, or (ii) when a resident has made a payment to a non-resident in Japan or in a foreign state, the resident

or non-resident in the case of (i), or the resident in the case of (ii) shall report such to the Minister of Finance, except cases specified by the Cabinet Order (*e.g.*, payment not exceeding JPY 30 million).[20]

Such mandatory reporting to the minister of finance for payment or receipt of payment exceeding JPY 30 million, such as between residents and non-residents or from a foreign state to Japan, does not leave out relevant transfers just because they are settled in virtual currency, since the intent of the law is to grasp any such transfer "identified as equivalents" of extinguishment of claims and obligations or as a transfer of value.

VI. PREPAID PAYMENT INSTRUMENTS

Digital tokens deemed not to constitute virtual currency may be considered "Prepaid Payment Instruments" depending on their characteristics.

Under the PSA, "Prepaid Payment Instruments" means any of the following:

i. Certificates, electronic devices, or other items ("Certificates, etc.") or numbers, markings, or other signs (including additions to the amount recorded in the Certificate by electronic or magnetic means in exchange for the receipt of consideration corresponding to the additional amount recorded) issued in exchange for the receipt of consideration corresponding to the amount (in cases where the amount is found each time to be converted to and indicated as an amount expressed in another unit, including the number of that unit; the same applies hereinafter) recorded in the Certificate or recorded using electronic or magnetic means (meaning in electronic form, magnetic form, or any other form that is impossible to perceive through the human senses alone; the same applies hereinafter), which can be used for the purpose of paying consideration for the purchase or leasing of goods or the receipt of provision of services from the issuer or the person designated by the issuer ("Issuer, etc.") by way of presentation, delivery, notification, or other means;

ii. Certificates, or numbers, markings, or other signs issued in exchange for the receipt of consideration corresponding to the quantity of goods or services recorded in the Certificate, etc. or recorded using electronic or magnetic means (including additions to the quantity of goods or services recorded in the Certificate, etc. by electronic or magnetic means in exchange for the receipt of consideration corresponding to the additional quantity recorded), which can be used for the purpose of claiming the delivery or provision of those goods or services from the Issuer, etc. by way of presentation, delivery, notification, or other means.

The above definitions are analyzed into the following three (3) elements: (a) property value typically in pecuniary amount is being recorded; (b) issued in exchange for the receipt of consideration corresponding to the amount; and (c) can be used for the purpose of paying consideration for the

20 Foreign Exchange and Foreign Trade Act, https://sherloc.unodc.org/cld/document/jpn/1949/foreign_exchange_and_foreign_trade_act.html?.

purchase or leasing of goods or the receipt of provision of services. Examples of Prepaid Payment Instruments include Suica, Web Money, and BitCash.

A. REGULATION OF PREPAID PAYMENT INSTRUMENTS

Prepaid Payment Instruments are divided into two categories: a) Prepaid Payment Instruments for Own Business and b) Prepaid Payment Instruments for Third-Party Business.

"Prepaid Payment Instruments for Own Business" means Prepaid Payment Instruments that can be used for the purpose of paying consideration for the purchase or leasing of goods or the receipt of provision of services solely from the issuer of Prepaid Payment Instruments (including persons who have a close relationship specified by Cabinet Office Order with that issuer ("Closely Related Persons")) or those Prepaid Payment Instruments that can be used for the purpose of claiming the delivery or provision of those goods or services only from the issuer of Prepaid Payment Instruments. "Prepaid Payment Instruments for Third-Party Business" means Prepaid Payment Instruments other than Prepaid Payment Instruments for Own Business.

Any person may issue Prepaid Payment Instruments for their Own Business. When the unused/outstanding balance as of March 31 and September 30 (such semi-annual dates are base dates) has exceeded the standard amount of JPY 10 million, the issuer must submit a written notice to the director-general of the relevant local finance bureau or local finance branch bureau. In contrast, no person may engage in the business of issuing Prepaid Payment Instruments for a Third-Party Business unless the person is a corporation registered with the director-general of the relevant local finance bureau or local finance branch bureau.

Those who are registered with respect to the Prepaid Payment Instruments for their Own Business and those who are registered in respect of the Prepaid Payment Instruments for a Third-Party Business are subject to the code of conduct rules for the Prepaid Payment Instruments (*e.g.*, Provision of Information on the issuer and the "Prepaid Payment Instruments", Making of Security Deposits for Issuance, Prohibition in principle of refunds to the holders of Prepaid Payment Instruments, Complaint Processing Measures, Information Security Management).

VII. OUTLOOK FOR VIRTUAL CURRENCY REGULATION IN JAPAN

The regulation of "virtual currency" in Japan was perceived as advanced and forward-looking when regulations were first published in 2016. However, a lot has happened since then, and regulatory framework has thus started to lag behind the fast-paced technological development.

As stated above, amendments to the PSA and FIEA regarding crypto assets will be tighter than those currently imposed. Further regulation, however, is not all bad. Some of the advantages include, amongst

others, increased market transparency due to clarity around consumer/investor protection requirements, the possibility of using ICOs and STOs for capital raising, and structuring and promiting the use of financial derivatives products utilizing crypto assets (e.g., crypto assets derivatives transactions).

In this way, the tightening of regulations may not necessarily hinder innovation; however, additional work remains to be done before the updates are completed.

TOKEN ALLIANCE

CHAMBER OF DIGITAL COMMERCE

UNDERSTANDING DIGITAL TOKENS

Legal Landscapes Governing Digital Tokens in the United Kingdom

Prepared by the Token Alliance – an industry initiative of the Chamber of Digital Commerce

SECOND EDITION • SEPTEMBER 2019

TABLE OF CONTENTS

II. REGULATORY OVERVIEW OF DIGITAL TOKEN MARKETS

I. INTRODUCTION

The regulation of digital tokens is a developing area as the current United Kingdom ("U.K.") financial services law was not developed with the use of digital tokens in mind. Over time new legislation may well be introduced (and interpretations of current legislation may change) to take account of the expected increase in the use of digital tokens, sharp and frequent price volatility of digital tokens and to safeguard the economy against the use of digital tokens (such as virtual currencies) for criminal purposes and intent. It also is important to bear in mind that subtle differences in the legal structure and commercial function of a digital asset can have significant regulatory consequences. It is not a "one size fits all" regime.

II. POTENTIAL LEGAL CLASSIFICATION AND RELATED REGULATORY CONSIDERATIONS

A. OVERVIEW

Broadly, there are several generic approaches to the regulation of digital tokens in the U.K. One is to treat them as a commodity or other form of physical property. Where this is the case, the marketing, purchase and sale of the digital token will largely be unregulated from a U.K. financial services law perspective, save if the contracts for the trading of the digital tokens fall within the scope of the U.K. law definitions of a derivative. Another is to treat them as a financial instrument (principally a security) but also possibly a unit in a fund (including a collective investment scheme, which is broadly defined

GENERIC REGULATORY APPROACHES TO TOKENS IN THE U.K.

1	2	3
A COMMODITY OR OTHER FORM OF PHYSICAL PROPERTY	A FINANCIAL INSTRUMENT	MONEY OR FORM OF CURRENCY

and capable of capturing arrangements involving digital tokens or an alternative investment fund), the third approach is to treat them as money or a currency (potentially e-money or entailing the provision of a payment service). In this regard, whether the digital token will be subject to regulation will depend on whether it is designed as a medium of exchange or whether it has more narrow functions such as solely enabling for the payment for services provided within the particular digital token's closed infrastructure.

The regulatory categorisation of the digital token is important as it will determine the extent to which (if at all) any U.K. authorisation, prospectus, marketing restrictions, systems, controls, procedural, conduct of business, anti-money laundering and anti-terrorist financing requirements apply.

B. U.K. COLLECTIVE INVESTMENT SCHEME ANALYSIS

The term "Collective Investment Scheme" ("CIS") is deliberately broad and vague and so it is capable of capturing a wide range of arrangements even if the parties to the arrangements do not intend to create or establish a 'fund' or a collective investment.

Section 235 of the Financial Services and Markets Act 2000 (as amended from time to time) ("FSMA") defines a CIS as "any arrangements with respect to property of any description . . . the purposes or effect of which is to enable persons taking part in the arrangements . . . 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."[1]

Further elements of the definition are that the participants do not have day-to-day control over the management of the property.[2]

In addition, the arrangements must have either of the following characteristics:[3]

1 Section 235 of FSMA.
2 *Id.*
3 *Id.*

» pooling of contributions and profits or income of the participants in the scheme (which would include the holders of the digital tokens); and

» the property is managed as a whole on behalf of the operator of the scheme.

Typically, a CIS takes in money from investors and invests it in some other type of property. It is that other property, plus any uninvested contributions and undisbursed profits and income, which would normally be regarded as the underlying property of the CIS.

In the context of digital tokens, arrangements are capable of being a treated as a CIS in circumstances where participants pay cash to an 'issuer' in exchange for a certificate or token which gives the participants/investors an entitlement to underlying property (e.g., gold, silver, wine, art, etc.) if the underlying property is managed by a third party (the term managed could entail administrative functions such as arranging for the property to be stored and/or insured) or if the contributions or profits of the participants/investors are pooled. Therefore arrangements relating to digital tokens need to be carefully scrutinised to determine whether they are within the U.K. CIS regime even if the intention is not to create a fund or collective investment.

Even if the arrangements fall within the basic definition of a CIS, they will not be caught if an exemption in the Schedule to the FSMA Collective Investment Scheme Order 2001 (the Order) applies. There are exemptions for arrangements relating to debt instruments, joint venture arrangements and those structured as bodies corporates.

The regulatory consequences of an arrangement relating to a digital token being a CIS are twofold:

» A CIS arrangement triggers authorisation requirements and compliance with certain rules for certain parties.

    For example, establishing, operating or winding up a CIS is a regulated activity under section 19 of FSMA and no exemption applies. This may be relevant to the person who is charged with establishing the arrangements, or arranging for the issuance of the certificates or tokens relating to digital tokens or arranging for the tokens to be stored and/or insured). Therefore, if this is done in the U.K., the operator will require authorisation from the U.K. Financial Conduct Authority (FCA). Other activities that may require authorisation, in relation to arrangements that amount to a CIS include managing investments, advising, dealing as principal or agent and arranging. It is an offence to carry on a regulated activity without authorisation under section 23 FSMA. Any contracts made by an unauthorised person (with participants/investors) in carrying on a regulated activity are unenforceable unless the court is satisfied that it is just and equitable to allow them to be enforced pursuant to section 28 of FSMA.

» A CIS arrangement will have an impact on the ability to market the CIS to investors in the U.K.

For example, it may only be possible to market the CIS to certain professional investors, high net worth individuals or certified sophisticated investors as units in a CIS are "controlled investments" under FSMA, and so section 21 and section 238 of FSMA will apply to their marketing.[4,5]

C. U.K. ALTERNATIVE INVESTMENT FUND ANALYSIS

An Alternative Investment Fund ("AIF") is defined in Article 4(1)(a) of the Alternative Investment Fund Managers Directive ("AIFMD") as any "collective undertaking including investment compartments thereof, which raises capital from a number of investors with a view to investing it in accordance with a defined investment policy and which is not required to be authorised under Article 5 of Directive 2009/65/EU" (the EU Directive dealing with authorisation of open ended retail funds). All elements of the AIF definition must be present in order for the digital token arrangements to be treated as an AIF.

An AIF is a particular type of fund or collective investment vehicle, which overlaps in certain respects with the definition of a CIS, but they are not exactly the same. For example, an arrangement structured as a closed ended body corporate is capable of being categorised as an AIF whereas such an entity would not be a CIS.

Arrangements that relate to body corporates, partnerships, unincorporated associations and a fund set up as a trust, which pool together capital raised from participants/investors for the purposes of investment (e.g., the pooled capital is used to purchase gold or silver) with a view to generating a pooled return for those investors from investments (e.g., the arrangements are capable of generating a return for the participants) may amount to an AIF.

An arrangement relating to digital tokens that meets the basic definition of an AIF under the AIFMD will not constitute an AIF if it falls within an exemption under Article 2 of the AIFMD. There are exemptions for holding companies, certain joint ventures and securitisation special purpose vehicles.

The regulatory consequences of an arrangement being an AIF may trigger a requirement for the manager to be authorised (known as the AIFM), the appointment of a depositary, and compliance with various procedures, controls, capital and conduct requirements. There are restrictions in relation to the marketing of AIFs, including the type of investors who can be marketed to, prior notifications to EU regulators and reliance on private placement rules.

4 Section 238(1) of FSMA restricts the marketing by authorized persons of an unregulated CIS unless it falls within one of the exemptions to this restriction (under FSMA (Promotion of Collective Investment Schemes) (Exemptions) Order 2001) (as amended) (the "CIS Promotion Exemptions Order") or under Chapter 4 of the Conduct of Business Sourcebook of the FCA Handbook.

5 Authorized persons may market unregulated CISs to certain categories of persons in the U.K. under the CIS Promotions Order, including, investment professionals (Article 14), certified high net worth individuals (Article 21), high net worth companies (Article 22), sophisticated investors (Article 23), self-certified sophisticated investors (Article 23a), associations of high net worth or sophisticated investors (Article 24).

D. U.K. E-MONEY ANALYSIS

E-money is defined in the Directive 2009/110/EC as electronically (including magnetically) stored monetary value represented by a claim on the electronic money issuer which: (i) is issued on receipt of funds for the purposes of making payment transactions; (ii) is accepted by a person other than the electronic money issuer; and (iii) is not otherwise excluded. The E-money directive is implemented in the U.K. through the Electronic Money Regulations 2011.

There is an explicit exclusion for monetary value stored in instruments that can be used to acquire goods or services only in the issuer's premises or under a commercial agreement with the electronic money issuer, either within a limited network of service providers or for a limited range of goods and services (the limited network exclusion) which may be relevant for arrangements involving digital tokens. The Payment Services Regulations 2017 introduced a notification obligation on firms relying on this exclusion where the total value of the payment transactions executed by the firm under the limited network exclusion exceeds € 1 million over a 12-month period.

In many instances, the digital token will not be treated as e-money because:[6]

- there is no claim against the issuer of the digital token for the value of the digital token acquired (indeed, in many instances, there will not even be an issuer);
- it does not have 'monetary value' (as it is not a currency); and
- the digital token is not issued on receipt of funds (e.g., assuming that the term "funds" means fiat currency, which is a term used to differentiate between "real currency" – meaning traditional currency such as USD, GBP, Euro, and Yen – from virtual currency).

However, the success of the digital token over time could alter how it is categorised from a regulatory perspective (e.g., it is accepted as a medium of exchange – i.e., currency – and therefore has monetary value).

If the digital token is e-money, this may require the issuer of e-money to be registered with the FCA, though there is a lighter touch regime for small e-money issuers. E-money issuers are subject to certain capital requirements, systems and controls, reporting and operational requirements.

E. U.K. PAYMENT SERVICES ANALYSIS

The Payment Services Directive ("PSD") regulates a broad range of services including those that enable: (i) cash to be placed on a payment account, (ii) cash withdrawals to be made from a payment account, (iii) the transfer of E-money; (iv) the execution of payment transactions where the funds are covered by a line of credit (e.g., direct debits, credit transfers), (v) customers to purchase goods and

6 Article 2(1) of the Electronic Money Regulations 2011, Article 2(1) of the Payment Services Regulations 2017 and Glossary of the UK FCA Handbook.

services through their online banking facilities or by e-money, and (vi) money remittance that does not involve the creation of payment accounts .

In many cases, the issuance as well as the purchase and sale of the digital token will not amount to the provision of a payment service subject to regulation under PSD, on the basis that the arrangements do not:

- enable cash to be placed on a payment account or cash withdrawals to be made;
- enable direct debits or credit transfers (e.g., standing orders) to be made;
- facilitate payment transactions where the funds are covered by a credit line since the digital token holders have to pay for the digital token upfront (i.e., they are pre-paid); and
- there are no money remittance services as funds are not received from a payer for the sole purpose of transferring a corresponding amount to a payee or to another payment service provider acting on behalf of the payee, and the funds are not received on behalf of, and made available to, the payee.

There is an exclusion for services based on specific payment instruments that can be used only in a limited way, which may be relevant in the context of digital tokens provided that they meet one of the following conditions:[7]

- they allow the holder to acquire goods or services only in the issuer's premises;
- they are issued by a professional issuer and allow the holder to acquire goods or services only within a limited network of service providers which have direct commercial agreements with the issuer;
- they may be used only to acquire a very limited range of goods or services; or
- they are valid only in a single EEA State, are provided at the request of an undertaking or a public sector entity, and are regulated by a national or regional public authority for specific social or tax purposes to acquire specific goods or services from suppliers, which have a commercial agreement with the issuer.

Those who provide payment services may be required to be authorised by the FCA and must comply with certain systems, controls and conduct requirements.

F. OTHER U.K. REGULATED ACTIVITIES ANALYSIS

Arrangements relating to digital tokens may entail the carrying on of a regulated activity. Section 19 of FSMA states that a person must not carry on a regulated activity in the U.K., or purport to do so, unless he is an authorised person or exempt person or an exclusion applies. This is referred to as the

7 Schedule 1, Part 2, 2(k) of the Payment Services Regulations 2017.

"general prohibition." Carrying on a regulated activity in breach of the general prohibition is a criminal offence and may result in certain agreements being unenforceable.

A regulated activity is described in FSMA as a specified activity that relates to a specified investment or property of any kind and is carried on by way of business (section 22, FSMA). Specified activities include dealing as principal or agent in a specified investment, making arrangements "with a view" to persons buying and selling certain specified investment, bringing about transactions in specified investments as well as safeguarding and administering tokens. Specified investments include shares, debt instruments, collective investment schemes, e-money and derivatives as defined in the FSMA ("Regulated Activities") Order 2001 ("RAO"). Whilst digital tokens are not specifically identified as a specified investment, the characteristics of the digital token would have to be assessed against the criteria of each specified investment to determine whether it is within scope.

In addition, any platform on which the digital tokens are traded or exchanged may be considered to be a regulated market, a multilateral trading facility or an organised trading facility if the digital token is categorised as a specified investment.

Even if a regulated activity is being performed, authorisation under FSMA may not be required if an exclusion is available. There are various exclusions in the RAO that may be relevant in the context of digital tokens including for overseas persons or whether the activity is carried out in connection with the sale of goods or the supply of services or there is an absence of holding out.

In the event of a regulated activity being performed and there is no available exclusion, there are three consequences to the digital token being categorised as a specified investment under the FSMA and the RAO as follows:

- the marketing of the digital token may be restricted under section 21 and/or section 238 of FSMA or subject to compliance with certain conduct rules;
- accessing the platform or exchange and its use by participants may be restricted; and
- the operator of the platform, the custodian of the digital tokens, the issuer of the digital token and those who make arrangements for others to acquire the digital tokens may be required to be authorised. This in turn would trigger the requirement to comply with certain capital, systems, controls and conduct requirements.

Even if the digital token is not categorised as a specified investment under FSMA and the RAO, the platform or exchange on which the digital token is bought or sold may be considered to be a commodity trading platform. It should be noted that there is no EU-wide regime for commodity trading platforms and so the analysis of whether a commodity trading platform needs to be regulated in a particular EU Member State will have to be considered on a country by country basis. A pure commodity platform would not currently be required to be regulated in the U.K. under FSMA.

G. REGISTRY, SETTLEMENT AND CLEARING

Many digital token systems will operate on a distributed ledger technology basis to register transfers of digital tokens between parties. As such, it is not considered likely that such a system will fall within the current boundaries of regulation in the U.K. However, systems which involve the transfer of digital tokens against value are being reviewed by a number of regulators including in the U.K. because of their resemblance to payment systems.

Digital token arrangements may also require a settlement system in order to transfer the digital token from one account or e-wallet to another and record the transaction pursuant to which the digital token is transferred and the movement of the corresponding "consideration." Indeed, if over time, the digital token becomes accepted as a medium of exchange for goods and services, then it may be necessary either to expand its registry system into a payment system or settlement system or to develop interoperability between the digital token settlement system and other virtual currency and/or fiat currency payment systems, which may result in it developing into a clearing system.

An entity which interposes itself between "counterparties" to certain types of contracts, thereby becoming the buyer to every seller and the seller to every buyer may be required to be authorised or registered as a central clearing party ("CCP"). This may be applicable to certain infrastructure arrangements involving digital tokens, depending on how they are categorised under the financial system. In the U.K., CCPs are supervised by the Bank of England and are subject to various capital, systems and controls, margin, and procedural requirements.

H. FUTURE U.K. REGULATORY DEVELOPMENTS (DATED AUGUST 2018)

European regulators, including the FCA, have recently issued warnings regarding the risks associated with investing in digital tokens such as bitcoin and ether. This has principally been driven by the recent volatility in the price of these virtual currencies. The FCA has warned investors that: (a) virtual currencies are not issued or guaranteed by a central bank or public authority; (b) virtual currencies do not have any legal status as a "fiat currency"; and (c) the purchase and sale of virtual currencies are not subject to safeguards and protections as they are unregulated in the U.K.[8]

The U.K. Government has signalled its intention to extend certain anti-money laundering and counter terrorist financing rules to virtual currency exchange platforms and certain custodial e-wallet providers through proposed changes to the EU Fourth Anti-Money Laundering Directive in the Fifth EU Anti-Money Laundering Directive.

If adopted, the Fifth EU Anti-Money Laundering Directive, which is expected to be agreed at the EU level this year, will require virtual currency exchange platforms and custodial e-wallet providers to

8 FCAWebsite: Consumer Warning about the risks in investing in cryptocurrency CFDs (dated 14/11/2017). FCA Website: Consumer warning abut the risks of Initial Coin Offerings (dated 12/09/2017).

conduct KYC due diligence checks on traders and users to determine their source of wealth and their source of income. Additional checks would be required if the trader or user is located in a "high risk" jurisdiction. In essence this will require virtual currency traders/users to disclose their identities and exchange platforms and e-wallet providers will be required to report any suspicious activity to the national crime agency.

Whether this will ultimately lead to virtual currencies and other digital tokens being subject to bespoke general regulatory rules which introduce authorisation requirements, prospectus-like disclosures, marketing restrictions, systems, controls, procedural, and conduct of business requirements remains to be seen. In a recent statement the FCA announced that it will be issuing joint guidelines (expected in late 2018) with the Bank of England on the possible future regulatory treatment of virtual currencies.

The FCA also recently stated that:

- "cryptocurrency derivatives are . . . capable of being treated as financial instruments under [MiFID II], although [the FCA] does not consider cryptocurrencies to be currencies or commodities for regulatory purposes . . . Firms conducting regulated activities in cryptocurrency derivatives must, therefore, comply with all applicable rules . . . and regulations;"[9] and
- it is "likely" that firms engaging in certain activities (e.g., dealing, arranging and advising) "in relation to derivatives that reference either cryptocurrencies or tokens issued through an initial coin offering (ICO), will require authorisation by the FCA."[10]

III. U.K. TAX ANALYSIS (UPDATED NOVEMBER 2019)

In this section, we explore key U.K. tax considerations that may arise on a distribution of utility tokens. This section does not explore tax issues attaching to the subscribers or acquirers of the tokens (other than in limited circumstances for certain employees).

Like many other jurisdictions, the United Kingdom has not introduced a special regime or specific rules for crypto assets. Therefore, the tax consequences of a token generation and distribution must be considered in light of general U.K. tax principles. The U.K. tax authority, H.M. Revenue and Customs, originally published guidance on 19 December 2018 in relation to the taxation of individuals who hold crypto assets.[11] This guidance was updated on 1 November 2019 to cover how H.M. Revenue and Customs will tax transactions undertaken by companies and other businesses involving crypto asset "exchange tokens"; this updated guidance does not address security or utility tokens.

9 https://www.fca.org.uk/news/statements/cryptocurrency-derivatives. The FCA does not provide a definition for "so-called cryptocurrencies".
10 Ibid.
11 https://www.gov.uk/government/publications/tax-on-cryptoassets.

When the U.K. launched its "Crytoassets Taskforce" consisting of H.M. Treasury, the Financial Conduct Authority and the Bank of England in March 2018, it concluded that there are three broad categories of crypto asset:[12]

1. **Exchange tokens –** which are often referred to as 'cryptocurrencies' such as Bitcoin, Litecoin and equivalents. These forms of token 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.

2. **Security tokens –** which amount to a 'specified investment' (see section F "Other U.K. Regulated Activities Analysis" in the U.K. regulatory comments above on page 12). 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 MiFID II.

3. **Utility tokens –** which can be redeemed for access to a specific product or service that is typically provided using a distributed ledger technology platform.

As mentioned above, this section explores how the U.K. rules apply in relation to utility tokens rather than security tokens (or the U.K.'s concept of "exchange tokens"), although there can be a certain degree of overlap between utility tokens and exchange tokens.

The analysis can be complex in relation to utility tokens primarily because of the uncertainty as to what exactly a utility token is (and most utility tokens differ in this respect).

This can be contrasted with the tax analysis of a security token (or even an "exchange token" now that the U.K. has published guidance concerning theem) because generally that analysis should be similar to reasonably well-understood tax analysis of a traditional security issuance.

A U.K. company can distribute utility tokens in a variety of ways. Thus, for the purposes of this section, the discussion assumes that the token sponsor is a U.K. company. Further, some U.K. businesses prefer to use an offshore vehicle to distribute utility tokens (rather than a U.K. company) because that can add a degree of simplicity to the numerous complications an onshore vehicle may bring. However, offshore vehicles have their own tax complications that need to be considered carefully (for example, ensuring that the tax residency of the offshore vehicle is not brought onshore, otherwise any perceived offshore benefits could be lost).

U.K. companies have four broad U.K. tax areas to consider when distributing utility tokens:

1. whether the distribution proceeds fall within the scope of corporation tax;

2. whether the distribution of the utility tokens triggers a value added tax ("VAT") charge;

12 https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/752070/cryptoassets_taskforce_final_report_final_web.pdf.

3. whether employment taxes (being income tax, national insurance (or social security) contributions, and the apprenticeship levy) are triggered by any tokens awarded to or acquired by employees; and

4. whether the utility tokens are subject to stamp duty or stamp duty reserve tax.

Each of these areas can create an absolute cost for a U.K. company or create a cash flow or funding cost to manage.

Although this section largely focuses on the tax implications of a token distribution, each of these taxes could arise at other points in the life cycle of a project (*e.g.,* set-up, token pre-sale, token sale, the operational phase, and any exit). Therefore, the best practice is to consider and plan for each phase at the outset.

Addressing some of the high-level aspects of each of these in turn:

1. CORPORATION TAX – TOKEN DISTRIBUTION PROCEEDS

In the United Kingdom, the profits of a company are currently (as of November 2019) subject to corporation tax at 19% (reducing to 17% in April 2020).[13]

As a broad starting point, the profit of a U.K. company is determined in accordance with accounting principles subject to various specific tax deviations. Therefore, it is important to understand the accounting treatment and how and when the accounts recognize any revenue from the token distribution because that will flow through to the tax analysis.

Once the tax analysis has been overlaid on the accounting treatment, the general proposition is that any token distribution proceeds received by a U.K. company for granting the tokens are likely to fall within the scope of U.K. corporation tax.

This means that 19% of the token distribution proceeds may need to be paid to the U.K. tax authority on account of corporation tax leaving the U.K. company with less cash than originally envisaged. The question then becomes whether a U.K. company has incurred any expenditure that can be used to offset any revenue received from the distribution to reduce any such leakage; this depends on the nature of the expenditure incurred by the U.K. company and also various other tax and accounting timing considerations. This is why it is important to understand any project's projected cash flow and proposed expenditure — these complications are one reason why an offshore entity situated in a low or no tax jurisdiction may afford an element of simplicity in this respect.

Further, it is important to build any anticipated tax leakage into the financial model at the outset so that no surprises manifest themselves at a later stage.

13 https://www.gov.uk/government/publications/rates-and-allowances-corporation-tax/rates-and-allowances-corporation-tax.

Other corporation tax issues of which to be mindful include:

A. *disposals of crypto assets:* as many token distributions accept payment by way of other crypto assets, it is possible for an exchange rate gain or loss to be made when the U.K. company eventually disposes of the relevant asset; and

B. *discounts / credits:* additional complications can arise where the token in question has an inbuilt discount for a future service or if it provides a service credit which can be used as a payment in kind — such complications are often linked to when revenue is recognized for accounting purposes.

2. VAT – TOKEN DISTRIBUTION PROCEEDS

VAT is an exceptionally broad tax and it captures effectively anything done (or granted) by a U.K. company in return for consideration. The distribution of utility tokens falls squarely within this scope because a U.K. company is distributing "tokens" in return for cash (or cryptocurrency) and, unlike the issuance of security tokens, there is no immediately obvious exemption from a VAT charge.

If VAT is chargeable, it can lead to an erosion of 20% of the token distribution proceeds; 20% is the current U.K. main rate of VAT.[14]

Even if there is no U.K. entity involved, VAT still needs to be considered where a non-U.K. entity distributes tokens to U.K. persons; this can be missed by overseas token sponsors who may assume that they do not need to be concerned with VAT.

U.K. VAT is based on European Union VAT law, so there should be similar issues arising in relation to every E.U. country. In addition, as many other jurisdictions have similar VAT systems, these (or equivalent) issues may arise elsewhere.

In relation to the application of VAT itself, there is limited guidance from the U.K. tax authority which provides very broadly that if the token is effectively like bitcoin, it should be treated as cash or currency (so the distribution or exchange of it ought to be exempt from VAT).[15]

Unfortunately, a significant proportion of utility tokens are not sufficiently comparable to bitcoin because various other rights attach to those tokens such as having the ability to claim a special discount, having an entitlement to other rights, or having a certain cash credit attached to them which can be applied against buying certain products or services.

Additional complexity may be caused depending on whether the tokens are distributed to consumers or businesses and whether the nature of the arrangements falls within specific

14 https://www.gov.uk/vat-rates.
15 *See* https://www.gov.uk/hmrc-internal-manuals/vat-finance-manual/vatfin2330; and https://www.gov.uk/government/publications/tax-on-cryptoassets/cryptoassets-tax-for-businesses.

identified categories of service, such as those relating to "electronically" supplied services which can engage other rules.

All of these factors could give rise to a token sponsor needing to register and account for VAT on any token distribution.

In light of this, companies can incorporate specific checks and balances in the token distribution process to ensure that the token sponsor has the necessary information required to undertake the VAT analysis.

Some of these complications may be eased by using an offshore structure. In addition, restricting the distribution of tokens to overseas business entities may help to shift the liability for any VAT to those entities.

Other VAT matters to consider include where a U.K. company pays for services with tokens (instead of with fiat) which is likely to give rise to VAT implications for both the U.K. company and the person providing services to the U.K. company (whether that person is an individual or a company).

3. EMPLOYMENT TAXES – DISTRIBUTION TO OR ACQUISITION BY EMPLOYEES

Employment tax implications arise in relation to utility token distributions, primarily where those tokens are distributed to or acquired by employees of a U.K. company.

Again, this is an area where, if the token is a security, the tax issues have a relatively clear analysis and there are available protections which can provide certainty and clarity.

Unfortunately, in the context of utility tokens, the position is much more opaque. The U.K. tax authority has now published guidance which addresses crypto assets received as earnings, but the guidance is vague in places and expressly states that different tax treatments may need to be adopted for utility and security tokens. The updated November 2019 guidance now addresses some of these issues but only in the context of "exchange tokens".[16]

Applying general U.K. tax principles typically leads to analysing whether the employee (or director) in question derives a benefit from their employment by virtue of the distribution or acquisition of the utility tokens.

If the answer is yes, the high-level analysis is that if the employee pays below market value for the tokens or is given them for free, there is likely to be an employment tax charge. Furthermore, given potential cash flow constraints of a U.K. company, this cash flow cost needs to be managed, modelled, and funded; for example, neither the U.K. company nor the employee

16 *See* Paying Employees in Cryptoassets, https://www.gov.uk/government/publications/tax-on-cryptoassets/cryptoassets-tax-for-businesses.

may have excess cash available to pay this tax.

To elaborate on this further, where an employee receives tokens as part of their employment, these rules will be engaged. This leads importantly to establishing whether the tokens can be considered to be "money's worth" which broadly means something that is of direct monetary value to the employee or something that is capable of being converted into money. In the guidance published by the U.K. tax authority, crypto assets received as employment income count as money's worth, suggesting that the U.K. tax authority will always consider this to be the case. It is still important to establish, however, whether the tokens can be considered to be money's worth.

What is or is not "money's worth" is an area guided by complex U.K. case law. The U.K. tax authority approaches this test by looking at what the arm's length market value of the tokens would be if they were sold to a third party at the time immediately after the employee acquired the asset.[17]

Therefore, sponsors may wish to consider obtaining a valuation from a professional valuation expert in relation to market value because it is inevitable that this will be an area of challenge from the U.K. tax authority in the years to come. Having professional advice in place regarding such valuations assists in minimising any risk. Complications also may arise in respect of valuations where pre-sales take place before the tokens are distributed or acquired. Any such pre-sale may give rise to an identifiable benchmark for the token valuation; if the employee has paid an amount below this benchmark, a tax charge could potentially arise.

This does not necessarily mean that it is correct to value any award or sale of tokens to employees in the same way as third-party benchmarks because various restrictions attaching to employee tokens could have an impact on their value. For example, indicators suggesting lower valuations potentially include distributing tokens to employees before any token sale begins, having restrictions preventing employees from disposing of the tokens for a number of years (lock-ups), and/or having tokens with forfeiture rights which apply if the employee leaves the business within a number of years or on bad terms.

If these rules are engaged, it is also important to establish whether the tokens are "readily convertible assets" or not; the importance of this goes to whether it is the employer and/or the employee that has various employment tax liabilities. Broadly, this turns on whether trading arrangements exist or are likely to come into existence at the point the crypto assets are distributed (which may often be the case). If the tokens are readily convertible assets, the responsibility for U.K. national insurance contributions and for withholding U.K. income tax on behalf of the employee falls on the employer.

17 https://www.gov.uk/hmrc-internal-manuals/employment-income-manual/eim00540.

As with the other tax aspects, the critical point is to consider and plan for these issues at the outset.

4. STAMP DUTY/STAMP DUTY RESERVE TAX

The United Kingdom imposes stamp duty and stamp duty reserve tax on certain transactions. Generally speaking these duties apply in respect of shares, loans, and various other securities and are levied at 0.5% of any consideration.

The positive news is that these duties are not typically relevant on a distribution or transfer of utility tokens. Where these taxes are more likely to arise in practice is where the token is a security token.

GLOBAL SUBJECT MATTER EXPERTS

The Chamber of Digital Commerce would like to express its gratitude to the following firms and individuals for authoring the country specific Sections contained in this report.

UNITED STATES:

Paul Atkins, Chief Executive Officer, Patomak Global Partners
John Cobb, Associate, Steptoe
Matthew Comstock, Partner, Murphy & McGonigle, P.C.
Michael Fletcher, Partner, RSM
Robert Greene, Strategic Advisor, Patomak Global Partners
Amy Davine Kim, Chief Policy Officer, Chamber of Digital Commerce
Kari Larsen, Counsel, Reed Smith LLP
Chelsea Parker, Blockchain Industry Analyst, Steptoe
Michael Selig, Associate, Perkins Coie LLP
Lisa Zarlenga, Partner, Steptoe

CANADA:

Paritosh Gambhir, Partner, KPMG
Ross McKee, Partner, Blakes
Stefania Zilinskas, Associate, Blakes

UNITED KINGDOM:

Potential Legal Classification and Related Regulatory Considerations:

Tim Dolan, Partner, Reed Smith LLP
Claude Brown, Partner, Reed Smith LLP
Karen Butler, Senior Associate, Reed Smith LLP

U.K. Tax Analysis:

Erin Becker, Dentons
Alex Tostevin, Dentons

AUSTRALIA:

Alex Cook, Lecturer, University of Western Australia Law School
Nick Giurietto, CEO and Managing Director, Australian Digital Commerce Association
Ivan Oshry, Head of Corporate, Kemp Strang
Ronald Tucker, Founder and President of the Board, Australian Digital Commerce Association
Michael Zheng, Senior Associate, Maddocks

GIBRALTAR:

Joey Garcia, Partner, ISOLAS LLP
Jonathan Garcia, Partner, ISOLAS LLP

JAPAN:

So Saito, So and Sato Law Offices
Tomoaki Katayama, So and Sato Law Offices