Legal Matters in Web 3: A Desk Reference

Editors

Anup Malani
Lee & Brena Freeman Professor

M. Todd Henderson
Michael J. Marks Professor of Law

The University of Chicago Law School
Chicago, Illinois

Table of Contents

Preface

This volume grew out of a conference on "Legal Matter in Web3" organized by Anup Malani and sponsored by the University of Chicago Law School in January 2023. Its aim was to convene leading practitioners to talk about the main legal case and controversies that Web3 firms were encountering. Coming soon after a series of crises, including the depeg of the Terra stablecoin and the collapse of the FTX Exchange, rocked Web3, the discussions were intense and productive.

At the end of the conference, at Malani's request, this volume's authors agreed to create a desk reference that could be used as an on-ramp for both lawyers to learn about Web3 and investors and managers in leading Web3 projects to learn about the main legal risks they face. Specifically, we asked some authors to address specific areas of law, e.g., securities regulation, commodities regulation, and the Bank Secrecy Act, that implicate a range of Web3 projects; and we asked others to address the range of legal issues that arise out of certain categories of Web3 projects or needs, e.g., raising capital, centralized exchanges, custodial services, and decentralized finance. There is necessarily some overlap between chapters. In general, Web3 project-oriented chapters in Part 1 provide a deep dive on those businesses and technologies, and sketch a range of legal risks associated with them; by contrast the chapters organized by legal areas in Part 2 provide a deeper dive on specific legal topics and use a range of projects to illustrate how they interest the Web3 ecosystem. We hope that the two approaches and Parts complement one another.

This volume would not have been possible without the contributions of many people. Foremost are the chapter authors, who generously contributed their time and expertise. As these are the leading lawyers in their respective fields on the topic, the value of this cannot be overstated. Each chapter was reviewed for content by peer attorneys. Authors revised their chapters in light of these reviewers' comments. Our excellent students— Denita Kiya, Karan Lala, Jane Ninivaggi, Flavio Pacheco, and Raam Tambe—made numerous contributions to specific chapters they were asked to edit. Malani also thanks Todd Henderson, a research collaborator and Law School colleague, who helped him edit submissions to this Desk Reference.

The success of the first Legal Matter in Web3 inspired a follow-on conference in January 2024. It was organized again by Malani, with help from Pat Daugherty and Katie Trkla, two of the authors in this Desk Reference. The second conference was sponsored by the Law School's Center on Law and Finance and Cornerstone Research. The events team at the University of Chicago Law School provided crucial logistical support at both conferences. Participants at both conferences indirectly enriched the

papers in this volume (and the field generally) through a series of high-caliber conversations with the authors of this volume. Thank you all.

Contributors

The following attorneys contributed chapters to this Desk Reference.

Patrick Daugherty, Partner
Foley & Lardner, LLP
Chicago, IL

Michael Frisch, Partner
Croke Fairchild Duarte & Beres
Chicago, IL

Bill Martin, Counsel
O'Melveny
New York, NY

Logan Payne, Counsel
Perkins Coie
Austin, TX

Greg Pesce, Partner
White & Case LLP
Chicago, IL

Kate Roin, Partner
Barlit Beck LLP
Chicago, IL

Kayvan Sadeghi, Partner
Jenner & Block LLP
New York, NY

Sarah Shtylman, Partner
Perkin Coie
Palo Alto, CA

Daniel Stabile, Partner
Winston & Strawn, LLP
Miami, FL

Scott Sugino, Partner
O'Melveny
Los Angeles, CA

Lilya Tessler, Partner
Sidley Austin LLP
Dallas, TX

Kathryn Trkla, Partner
Foley & Lardner, LLP
Chicago, IL

The following attorneys reviewed or edited chapters in this Desk Reference.

Olta Andoni, General Counsel
Enclave Markets
Chicago, IL

Lewis Rinaudo Cohen, Partner
Cahill Gordon & Reindel LLP
New York, NY

Carl Fornaris, Partner
Winston & Strawn LLP
Miami, FL

Michelle Ann Gitlitz, General Counsel
Flexa Inc.
New York, NY

Louis B. Goldman, Managing Partner
Navigator Law Group LLC
Chicago, IL

Todd Henderson, Professor
University of Chicago Law School
Chicago, IL

Kimberly A. Prior, Partner
Winston & Strawn LLP
Miami, FL

Karan Lala, Student
University of Chicago Law School
Chicago, IL

Denita Kiya, Student
University of Chicago Law School
Chicago, IL

Jane Ninivaggi, Associate
Sullivan & Cromwell LLP
New York, NY

Flavio Pacheco, Student
University of Chicago Law School
Chicago, IL

Raam Tambe, Student
University of Chicago Law School
Chicago, IL

Part 1: Project Perspectives

Decentralized Finance (DeFi)

Kayvan Sadeghi*

A. Introduction

Decentralized finance, or DeFi, sits at the intersection of blockchain and financial services.1 It is an umbrella term intended to capture a variety of financial applications that offer potential to reshape the boundaries of traditional financial markets. For the same reason, DeFi cuts across a multitude of regulatory regimes, including those governing securities, commodities, payment instruments, and others. To address the myriad legal complexities, one must first have a basic understanding of what DeFi does and how DeFi does it (*i.e.*, the technology underlying DeFi and the markets in which it operates). Accordingly, this Chapter provides an overview of DeFi from a technical, commercial, and legal perspective.

There is no single accepted definition of DeFi,[2] but the term is generally used to describe an emerging ecosystem of financial products and services intended to operate free from (or with reduced reliance upon) intermediaries and central authorities, and instead based on a decentralized environment of public, permissionless blockchains.[3] Disintermediation is typically achieved through non-custodial financial products and services encoded in open-source software protocols, which run on permissionless blockchains to allow for various forms of automated peer-to-peer (P2P) transactions.[4]

---

* Sadeghi is a Partner at Jenner & Block in New York, NY (https://www.jenner.com/en/people/kayvan-b-sadeghi). Sadeghi thanks Peter Nadimi, General Counsel at Aptos, and Shailee Sharma, an associate, at Jenner & Block for their comments. This chapter is the work-product of Jenner & Block. Olta Andoni, General Counsel at Enclave Markets, reviewed this chapter.

[1] Wharton Blockchain and Digital Asset Project & World Economic Forum, *DeFi Beyond the Hype—The Emerging World of Decentralized Finance* 1 (May 2021).

[2] U.S. Dep't of the Treasury, *Illicit Finance Risk Assessment of Decentralized Finance* 1 (Apr. 2023), available at https://home.treasury.gov/news/press-releases/jy1391.

[3] *See, e.g.*, Reiff, Nathan, "A Brief History of DeFi," *Decrypt* (Feb. 9, 2023), available at https://decrypt.co/resources/a-brief-history-of-defi-learn; Wharton Blockchain and Digital Asset Project & World Economic Forum, *DeFi Beyond the Hype—The Emerging World of Decentralized Finance* 1 (May 2021).

[4] Wharton Blockchain and Digital Asset Project & World Economic Forum, *DeFi Beyond the Hype—The Emerging World of Decentralized Finance* 1 (May 2021); U.S. Dep't of the Treasury, *Illicit Finance Risk*

DeFi platforms facilitate purchasing or trading a wide variety of assets, lending and borrowing, and payments, among other functions.[5] These functions can be applied to a wide variety of tokens that may be characterized as securities, commodities, derivatives, collectibles, or other more complex financial products,[6] potentially implicating a host of separate and overlapping regulatory regimes.

Despite its name, the term DeFi is often used loosely to include a variety of blockchain-based financial products and services that are not functionally decentralized.[7] Although DeFi platforms may purport to run autonomously, and/or to rely on distributed governance structures in which users make decisions collectively, many DeFi services have a controlling organization or group that provides a measure of centralized administration and governance.[8] "The degree to which a purported DeFi service is in reality decentralized is a matter of facts and circumstances."[9]

As used in this Chapter, DeFi products and services typically have or purport to have certain distinguishing features, including that they:

- Mediate the transfer and exchange of value;
- Offer trustless or at least trust-minimized operation and settlement, *i.e.* transactions are executed and recorded automatically according to the rules of the protocol, typically on public, permissionless blockchains;
- Have a non-custodial design, so that users retain control of their assets, which cannot—in theory—be unilaterally expropriated or modified by third parties, including intermediaries or other service providers; and
- Provide open-source code and interoperability so that their functionality can be composed together with other DeFi products or services.[10]

In practice, many products and services construed as DeFi begin as centralized projects and exist on a spectrum between centralized control and decentralization and/or

---

Assessment of Decentralized Finance 1 (Apr. 2023), available at https://home.treasury.gov/news/press-releases/jy1391.

[5] Carapella, Fracesca, et al, "DeFi: Transformative Potential and Associated Risks," Federal Reserve Bank of Atlanta's Policy Hub, No. 14-2022 at 8 (Oct. 2022).

[6] U.S. Dep't of the Treasury, *Illicit Finance Risk Assessment of Decentralized Finance* 8 (Apr. 2023), available at https://home.treasury.gov/news/press-releases/jy1391; Wharton Blockchain and Digital Asset Project & World Economic Forum, *DeFi Beyond the Hype—The Emerging World of Decentralized Finance* 2 (May 2021).

[7] U.S. Dep't of the Treasury, *Illicit Finance Risk Assessment of Decentralized Finance* 1 (Apr. 2023), available at https://home.treasury.gov/news/press-releases/jy1391.

[8] *Id.*

[9] *Id.*

[10] Wharton Blockchain and Digital Asset Project & World Economic Forum, *DeFi Beyond the Hype—The Emerging World of Decentralized Finance* 3-4 (May 2021).

automation, with a professed goal ultimately to reach a fully decentralized and/or automated state.[11]

B. DeFi Market Structure and Use Cases

The roots of DeFi trace back to the advent of Bitcoin in 2009, which was introduced as a decentralized digital currency.[12] Thus, payments is arguably the first envisioned use case for decentralized finance. A few years later, the launch of the Ethereum blockchain laid the foundation for DeFi as we know it today.[13] Decentralized financial applications were among the earliest use cases of the Ethereum blockchain.[14] Over time, DeFi platforms have evolved to offer a wide range of financial services, with different protocols serving different financial purposes and investment strategies, and segments of the market.[15] Determining how each platform may be regulated depends both on the nature of the financial service (*i.e.*, borrowing, trading, etc.), as well as how the underlying assets are characterized (*i.e.*, as commodities, securities, derivatives, etc.).

Stablecoins. One of the earliest DeFi protocols, MakerDAO, began to take shape in late 2014 and introduced the eDollar on a testnet for the Ethereum blockchain in 2015.[16] It evolved into what we know as MakerDAO today, which enables users to deposit ETH (and other assets) as collateral for generating the stablecoin Dai.[17]

Borrowing and lending. In addition to creating a stablecoin for payments, the process by which users of Maker could generate Dai has similarities to taking out an overcollateralized loan.[18] It provided a means to monetize ETH by borrowing against it, without selling the ETH or foregoing any future appreciation in the price of ETH, because the user could recover their initial ETH deposit by returning the amount of Dai they had "borrowed."[19] By 2017, Maker had emerged as a prominent borrowing

---

[11] World Economic Forum & Wharton Blockchain and Digital Asset Project, *Decentralized Finance (DeFi) Policy-Maker Toolkit* 9 (June 2021).

[12] The term DeFi, however, was not coined until August 2018 in a Telegram chat between Ethereum developers and entrepreneurs.

[13] *See, e.g.*, Reiff, Nathan, "A Brief History of DeFi," *Decrypt* (Feb. 9, 2023), available at https://decrypt.co/resources/a-brief-history-of-defi-learn. The Ethereum blockchain was introduced in 2013 white paper entitled "A Next-Generation Smart Contract and Decentralized Application Platform." MakerDAO, *A Brief History of DeFi* (Mar. 12, 2021), available at https://blog.makerdao.com/a-brief-history-of-decentralized-finance-defi/.

[14] *Id.*

[15] *Id.*

[16] *Id.*

[17] Reiff, Nathan, "A Brief History of DeFi," *Decrypt* (Feb. 9, 2023), available at https://decrypt.co/resources/a-brief-history-of-defi-learn.

[18] Markov, Igor & Antoinette Schoar, *Cryptocurrencies and Decentralized Finance*, BIS Working Papers No 1061 24 (Dec. 2022), available at https://www.bis.org/publ/work1061.pdf.

[19] MakerDAO, "The Maker Protocol: MakerDAO's Multi-Collateral Dai (MCD) System, available at https://makerdao.com/en/whitepaper/#the-dai-stablecoin.

protocol.[20] Other protocols also emerged around that time to offer various permutations of borrowing and lending, including Aave and Compound.[21]

DeFi lending protocols typically do not conduct credit checks or have any process for evaluating any approving borrowers (though they may block users on sanctions lists or from certain jurisdictions).[22] As a result, to maintain financial viability DeFi lending protocols typically require overcollateralization, meaning that borrowers must deposit more assets as collateral than the value of the loan they wish to borrow.[23] This approach mitigates the risk of default and prevents a loss to the protocol in the event of default.[24]

Trading. Another early use case for decentralized finance was trading tokens.[25] Some early projects (such as EtherDelta) enabled trading based on a peer-to-peer exchange model, to match buyers and sellers in a fashion somewhat comparable to order books underlying exchanges in traditional financial markets.[26] In 2017, however, Bancor introduced a decentralized exchange (DEX) on Ethereum structured as an automated market maker ("AMM", discussed further below), in which trades take place between the user and a pool of assets (peer-to-pool), rather than matching a buyer and seller (peer-to-peer).[27] Users could also deposit assets into the pools of assets used for trading and thereby receive a share of the trading fees.[28]

The AMM model quickly gained prominence, with numerous additional DEXs emerging based on similar AMM models, including Uniswap, Sushiswap, and many others. In 2021, the volume of crypto assets in the top six AMM-based DEXs was estimated to exceed $15 billion,[29] and the total transaction volume was estimated to be well in excess of $100 billion per month.[30]

---

[20] *See, e.g.*, Reiff, Nathan, "A Brief History of DeFi," *Decrypt* (Feb. 9, 2023), available at https://decrypt.co/resources/a-brief-history-of-defi-learn.

[21] Schar, Fabian, "DeCentralized Finance: On Block- and Smart Contract-Based Financial Markets," Fed. Reserve Bank of St. Louis Review 165 (2Q 2021).

[22] Xu, Jiahua & Nikhil Vadgama, "From banks to DeFi: the evolution of the lending market," *University College London, Centre for Blockchain Technologies* 6 (Dec. 20, 2022), available at https://arxiv.org/pdf/2104.00970.pdf.

[23] Markov, Igor & Antoinette Schoar, *Cryptocurrencies and Decentralized Finance*, BIS Working Papers No 1061 37 (Dec. 2022), available at https://www.bis.org/publ/work1061.pdf.

[24] Schar, Fabian, "DeCentralized Finance: On Block- and Smart Contract-Based Financial Markets," Fed. Reserve Bank of St. Louis Review 165 (2Q 2021).

[25] Carapella, Fracesca, et al, "DeFi: Transformative Potential and Associated Risks," *Federal Reserve Bank of Atlanta's Policy Hub*, No. 14-2022 at 11-12 (Oct. 2022).

[26] Lin, Lindsay, X., "Deconstructing Decentralized Exchanges," *Stanford Journal of Blockchain Law & Policy* (2019), available at https://stanford-jblp.pubpub.org/pub/deconstructing-dex.

[27] Xu, Jiahua, et al., "SoK: Decentralized Exchanges (DEX) with Automated Market Maker (AMM) protocols" (Apr. 19, 2021), available at https://berkeley-defi.github.io/assets/material/DEX%20with%20AMM%20Protocols.pdf.

[28] *Id.*

[29] *Id.*

[30] Markov, Igor & Antoinette Schoar, *Cryptocurrencies and Decentralized Finance*, BIS Working Papers No 1061 37 (Dec. 2022), available at https://www.bis.org/publ/work1061.pdf.

Yield farming and asset management. The process of placing assets into DeFi protocols to earn yield (in the form of interest or a share of protocol transaction fees, newly issued tokens, or a series of more complex strategies), came to be commonly referred to as "yield farming."[31] Protocols like Yearn simplified the process of maximizing yield from disparate DeFi protocols, effectively providing a form of asset management service.[32] These services contributed to an explosion of interest and development in DeFi in 2020 that was commonly referred to as "DeFi summer."[33]

As the DeFi ecosystem continues to grow, other use cases have emerged including prediction markets or decentralized betting;[34] synthetic assets (which are representations of real-world assets without holding the underlying asset);[35] among many others.

Governance. Many DeFi platforms operate as decentralized autonomous organizations (DAOs).[36] DAOs are self-governing entities operating on smart contracts and governed by the collective decisions of their token holders.[37] These organizations are designed to operate transparently and autonomously, minimizing the need for centralized authority.[38]

Any participant with governance tokens can propose changes, upgrades, or modifications to the DeFi platform.[39] These proposals can range from technical improvements to changes in protocol parameters or even alterations to the tokenomics.[40] Once a proposal is submitted, token holders can cast their votes to signal their support or opposition to the suggested change.[41] To ensure effective governance and prevent malicious actions, some DeFi platforms implement quorum requirements and voting thresholds.[42] Quorum represents the minimum percentage of total tokens

---

[31] Wharton Blockchain and Digital Asset Project & World Economic Forum, *DeFi Beyond the Hype—The Emerging World of Decentralized Finance* 5 (May 2021).
[32] Dale, Brady, "With COMP Below $100, a Look Back at the 'DeFi Summer' it Sparked," *CoinDesk* (Oct. 20, 2020), available at https://www.coindesk.com/business/2020/10/20/with-comp-below-100-a-look-back-at-the-defi-summer-it-sparked/.
[33] *Id.*
[34] *See, e.g.*, Augur, https://www.augur.net/.
[35] *See, e.g.*, Synthetix, https://synthetix.io/.
[36] Makarov, Igor & Antoinette Schoar, *Brookings Papers on Economic Activity*, "Cryptocurrencies and Decentralized Finance (DeFi)" 35 (Mar. 24, 2022), available at https://www.brookings.edu/wp-content/uploads/2022/03/SP22_BPEA_MakarovSchoar_conf-draft.pdf.
[37] *Id.*
[38] *Id.*
[39] *Id.*; Wharton Blockchain and Digital Asset Project & World Economic Forum, *DeFi Beyond the Hype—The Emerging World of Decentralized Finance* 6 (May 2021).
[40] Makarov, Igor & Antoinette Schoar, *Brookings Papers on Economic Activity*, "Cryptocurrencies and Decentralized Finance (DeFi)" 35 (Mar. 24, 2022), available at https://www.brookings.edu/wp-content/uploads/2022/03/SP22_BPEA_MakarovSchoar_conf-draft.pdf.
[41] *Id.*
[42] *Id.*

that must be used in voting to consider a proposal val*Id*.[43] Thresholds indicate the minimum percentage of approval votes needed for a proposal to be accepted.[44]

Proponents of decentralized governance point to its benefits, including decentralization and inclusivity, flexibility and adaptability, and transparency and accountability, which foster a fair and efficient decision-making process in the DeFi ecosystem.[45] But there are also risks associated with such governance, including challenges in coordinating and encouraging broad user participation, the potential for security and governance attacks from malicious actors, and the legal and regulatory complexities arising from its decentralized nature.[46]

C. DeFi Infrastructure

1. A Composable System of Money Legos

DeFi protocols are often compared with Lego pieces or referred to as "money legos" by virtue of their ability to interoperate with each other to form new and more complex financial products and services.[47] This flexibility allows for an ever-expanding range of possibilities and unprecedented interest in open financial engineering.[48] It also gives rise to a host of legal complications.[49]

The interoperability of DeFi is impacted by both the "tech stack" and the composability of each component. Tech stacks refer to the layers of technology infrastructure and software that work together to enable the operation of DeFi

---

[43] World Economic Forum & Wharton Blockchain and Digital Asset Project, "Decentralized Autonomous Organization Toolkit" 15 (Jan. 2023), available at https://www3.weforum.org/docs/WEF_Decentralized_Autonomous_Organizations_Beyond_the_Hype_2022.pdf; OECD, "Why Decentralized Finance (DeFi) Matters and the Policy Implications" 33-34 (2022), available at https://www.oecd.org/daf/fin/financial-markets/Why-Decentralised-Finance-DeFi-Matters-and-the-Policy-Implications.pdf.

[44] Makarov, Igor & Antoinette Schoar, *Brookings Papers on Economic Activity*, "Cryptocurrencies and Decentralized Finance (DeFi)" 35 (Mar. 24, 2022), available at https://www.brookings.edu/wp-content/uploads/2022/03/SP22_BPEA_MakarovSchoar_conf-draft.pdf.

[45] Wharton Blockchain and Digital Asset Project & World Economic Forum, *DeFi Beyond the Hype—The Emerging World of Decentralized Finance* 5 (May 2021); Binance Academy, "What are Governance Tokens?" (Jun. 13, 2022), available at https://academy.binance.com/en/articles/what-are-governance-tokens.

[46] OECD, "Why Decentralized Finance (DeFi) Matters and the Policy Implications" 34 (2022), available at https://www.oecd.org/daf/fin/financial-markets/Why-Decentralised-Finance-DeFi-Matters-and-the-Policy-Implications.pdf.

[47] Financial Stability Board, "The Financial Stability Risks of Decentralized Finance" 21 (Feb. 16, 2023).

[48] Schar, Fabian, "DeCentralized Finance: On Block- and Smart Contract-Based Financial Markets" 169 (2Q 2021); OECD, "Why Decentralized Finance (DeFi) Matters and the Policy Implications" 33-34 (2022), available at https://www.oecd.org/daf/fin/financial-markets/Why-Decentralised-Finance-DeFi-Matters-and-the-Policy-Implications.pdf.

[49] *Id.*

platforms.[50] Composability, on the other hand, pertains to the ability of different DeFi protocols and smart contracts to interact with each other to create new financial products and services.[51]

Tech stacks in DeFi typically involve multiple layers, including the underlying blockchain protocol layer, a layer of smart contracts running on that underlying blockchain protocol, a user-interface or application layer that facilitates user interaction with the on-chain smart contracts, and a user's wallet software.[52]

The blockchain layer serves as the foundational layer, where the decentralized ledger and consensus mechanisms reside.[53] Ethereum is one of the most widely used blockchain platforms in DeFi, but many other blockchains have a robust suite of DeFi applications as well.[54] In addition, as discussed above, many blockchain ecosystems are now comprised of what are referred to as Layer-1 and Layer-2 blockchains.[55]

Deployed on the blockchain layer, smart contracts are programmable code that automatically execute predefined actions when specific conditions are met.[56] These smart contracts enable DeFi protocols to perform various financial functions such as lending, borrowing, trading, and asset management.[57] They provide the logic and rules for DeFi applications to function autonomously and transparently, without relying on centralized authorities.[58]

Next, the application layer comprises the smartphone apps and website user interfaces that provide the user experience (UX) elements to facilitate interaction with DeFi smart contracts.[59] Finally, most user interfaces are designed to interact with separate third-party wallet providers, which are the last layer of the tech stack through which the user controls the private keys to their blockchain addresses.[60]

2. Types of Assets in DeFi

DeFi offers different asset classes that form the foundation of its innovative ecosystem. Tokens, which can be any form of token throughout the blockchain space, which could be tokens native to a particular protocol (BTC, ETH), or fungible or non-fungible tokens governed by smart contracts deployed on one or more existing

---

[50] *Id. at* 155.
[51] *Id. at* 168-169.
[52] *Id. at* 155-156.
[53] *Id.*
[54] *Id. at* 157-158.
[55] *Id.*
[56] Carapella, Fracesca, et al, "DeFi: Transformative Potential and Associated Risks," *Federal Reserve Bank of Atlanta's Policy Hub*, No. 14-2022 at 6 (Oct. 2022).
[57] *Id.*
[58] *Id.*
[59] Schar, Fabian, "DeCentralized Finance: On Block- and Smart Contract-Based Financial Markets" 156 (2Q 2021).
[60] *Id.*

protocols (DAI, etc.).[61] Depending on the nature of the tokens, could be securities, commodities, derivatives, collectibles. For purposes of the discussion here, a few types of tokens are worthy of note for their prominence in DeFi applications.

Liquidity Pool ("LP") Tokens. LP tokens are a fundamental building block of the DeFi ecosystem. In DeFi, liquidity pools are the pool of assets held in smart contracts as the basis for borrowing and lending, and for DEX trading in AMM models.[62] The liquidity for these DeFi protocols is provided by the users, and LP tokens function almost as a "claim check."[63] When users deposit assets into a liquidity pool, they receive LP tokens in proportion to the amount of pool they contributed, enabling the user to recover their respective share of the liquidity pool.[64] The value and composition of the pool may have changed in the interim as a result of other users trading into and out of the pool, along with the accumulation of related fees.[65] Thus, by holding liquidity pool tokens, users can earn yield in the form of trading fees accumulating in the pool.[66]

Beyond serving as proof of ownership of a pro rata share of the liquidity pool, LP tokens can generally be freely traded or transferred,[67] making them a distinct, liquid asset class in the DeFi landscape.

Governance Tokens. Many leading DeFi protocols are, or purport to be, governed by DAOs and have issued "governance tokens" enabling users to participate in that governance. Prominent examples include Compound (which described itself as a money market protocol),[68] and Yearn (an aggregator service designed to help users maximize the yield they generated from other DeFi protocols),[69] both of which launched tokens in 2020, contributing to the DeFi Summer.

Governance tokens may not, and often do not, convey any direct economic benefit, but they can be traded in the secondary market where they often trade at substantial value.[70] Instead, they enable the holder to participate in governance of the project by voting on certain proposals that impact the function of the protocol (and thus were called "governance tokens").[71] The right to participate in governance has led some to

---

[61] Wharton Blockchain and Digital Asset Project & World Economic Forum, *DeFi Beyond the Hype—The Emerging World of Decentralized Finance* 5 (May 2021).
[62] U.S. Dep't of the Treasury, *Illicit Finance Risk Assessment of Decentralized Finance* 11 (Apr. 2023), available at https://home.treasury.gov/news/press-releases/jy1391.
[63] *Id.*
[64] *Id.*
[65] *Id.*
[66] *Id. at* 10.
[67] *Id. at* 10-11.
[68] Compound Finance, "Compound: The Money Market Protocol" 8 (Feb. 2019), available at https://docs.compound.finance/v2/governance/.
[69] Yearn Finance, "Using Yearn," available at https://docs.yearn.finance/getting-started/using-yearn.
[70] Chainalysis, "Dissecting the DAO: Web3 Ownership is Surprisingly Concentrated" (June 27, 2022), available at https://blog.chainalysis.com/reports/web3-daos-2022/.
[71] *Id.*

analogize governance tokens to equity securities, while others have asserted that they represent an interest in a partnership, unincorporated association, or similar entity.

Wrapped Assets. Wrapped assets are tokens representing other tokens, including tokens that may reside natively on different blockchains.[72] For example, Wrapped Bitcoin (WBTC) represents Bitcoin on the Ethereum blockchain, allowing users to effectively deploy Bitcoin in DeFi applications on the Ethereum network.[73] While WBTC is intended to serve as an equivalent to BTC from an economic perspective, it is not necessarily clear that the two would always be treated the same way from a legal perspective.

Stablecoins. Stablecoins represent a crucial asset class within the DeFi ecosystem, as they provide the means by which DeFi users can move between exposure to crypto assets and traditional fiat currencies.[74] There are several types of stablecoins, which may receive different legal treatment:

- Fiat-Backed Stablecoins:[75] These stablecoins are typically pegged to traditional fiat currencies like the U.S dollar, Euro, or Japanese Yen, and backed by (or purport to be backed by) reserves of the pegged currency or other cash equivalents. Examples include USD Coin (USDC) and Tether (USDT).[76]

- Crypto-Backed Stablecoins:[77] Crypto-backed stablecoins are collateralized by other cryptocurrencies. DAI, for example, is pegged to the U.S dollar but backed by a reserve of ETH or other assets.[78] Smart contracts control the supply of stablecoins based on the value of the underlying collateral and facilitate the liquidation of that collateral when necessary to maintain the peg.[79]

- Algorithmic Stablecoins:[80] Algorithmic stablecoins rely on algorithms, rather than stable collateral, to hold a stable price. They typically seek to do so by adjusting the supply in response to changes in demand in an effort to maintain

---

[72] U.S. Dep't of Treasury, "Action Plan to Address Illicit Financing Risks of Digital Assets" 6 fn. 19, available at https://home.treasury.gov/system/files/136/Digital-Asset-Action-Plan.pdf.
[73] *See* WBTC, https://wbtc.network/.
[74] President's Working Group on Financial Markets, et al., "Report on Stablecoins" 1 (Nov. 2021), available at Report on Stablecoins (treasury.gov).
[75] *Id. at* 2.
[76] Liberty Street Economics, "Runs on Stablecoins," Fed. Reserve Bank of New York (July 12, 2023), available at https://libertystreeteconomics.newyorkfed.org/2023/07/runs-on-stablecoins/#:~:text=Source%3A%20CoinMarketCap.-,The%20Different%20Types%20of%20Stablecoins,backed%20by%20traditional%20financial%20assets.
[77] *Id.*
[78] *Id.*
[79] *Id.*
[80] *Id.*

equilibrium.[81] Many such tokens have failed, calling into question whether it is possible to create a truly stable algorithmic stablecoin.[82]

3. Automated Market Makers (AMMs)

AMMs are a critical component of the DeFi ecosystem, enabling seamless and permissionless trading of digital assets through liquidity pools.[83] Many of the best known DEXs have relied on some form of AMM model, including Uniswap, Sushiswap, Pancake Swap, LiquidSwap, KyberSwap, Balancer, Bancor, Curve, and many others.[84]

Unlike traditional exchanges that use an order book to bring together buyers and sellers, AMMs accumulate pools of assets and allow users to trade assets against the pool without need of any corresponding counterparty on the other side of the trade.[85] To do so, AMMs incorporate mathematical algorithms to determine exchange ratios between the assets in the liquidity pool(s), and dynamically adjust the relative prices as the balance of assets in the pool changes in response to supply and demand.[86] The constant availability of liquidity promotes a more active and liquid trading environment.[87]

The AMM structure is relevant from a legal perspective in several ways. First, it does not follow the conventional conception of an exchange, in that it does not rely on an order book to bring buyers and sellers together and match orders, calling into question its status under existing laws.[88] Second, it presents different risks than a conventional exchange. The automated algorithmic pricing mechanism may avoid certain risks attendant to a typical order book model (spoofing and the like), but the presence of a large pool of liquidity presents an appealing target to hackers (or ill-intentioned founders), and thus raises distinct security concerns.[89]

---

[81] *Id.*
[82] *Id.*
[83] Xu, Jiahua, et al., "SoK: Decentralized Exchanges (DEX) with Automated Market Maker (AMM) protocols" (Apr. 19, 2021), available at https://berkeley-defi.github.io/assets/material/DEX%20with%20AMM%20Protocols.pdf.
[84] *Id.*
[85] *Id.*
[86] *Id.*
[87] *Id.*
[88] *Id.*
[89] *Id.*

4. Privacy and mixers

In the DeFi ecosystem, privacy and mixers address the delicate balance between transparency and anonymity.[90] Blockchain technology inherently offers a measure of transparency by recording all transactions on a public ledger, and therefore privacy measures are necessary if one wishes to maintain any measure of privacy over their financial transactions.

Privacy solutions in DeFi take many forms. One such form is known as a mixer, or tumbler. Mixers obfuscate the origin and destination of crypto asset transactions by allowing a user to send assets into a pool of assets that is combined with the assets of other senders, and then to direct the pool to send an equivalent value of crypto assets out of the pool to the destinations of the user's choice.[91] The transactions are often split into multiple separate smaller transactions, further complicating the ability to match any particular inbound transaction to any particular outbound transaction.[92] This process makes it challenging to trace the flow of funds.

Mixers have both legitimate and illegitimate use cases. If, for example, someone were to receive a large amount of crypto assets to an address publicly affiliated with their identity, they may have legitimate concerns for their personal safety. Mixers allow a user to dispose of the funds in their publicly affiliated address, so that anyone later checking the known wallet address would not know whether or where they held any remaining amount of crypto assets.

While privacy and mixers offer significant benefits, they also introduce potential risks. The anonymity provided by mixers may attract illicit activities, such as those seeking to evade sanctions or other financial crime laws. The legal ramifications of a tool like this with powerful applications for both legitimate and illegitimate use cases, is currently playing out in the courts as discussed further below in Section D.1.

D. Legal Considerations and Authority

DeFi introduces unique legal intricacies because much of the legal framework for our traditional financial system is organized around distinct asset classes (*i.e.*, commodities or securities) based on their historically separate marketplaces, and dependent upon regulating the intermediaries that facilitate transactions in those markets (*i.e.* the exchanges, brokers, and the like). Instead of fitting neatly into traditional categories, DeFi overlaps and blurs the lines, necessitating a multi-faceted legal and regulatory approach. It also does not share the intermediated structure of traditional financial markets—replacing that structure with a technology stack

---

[90] Wang, Zhipeng et al., "On How Zero-Knowledge Proof Blockchain Mixers Improve, and Worsen User Privacy" 1 (Mar. 6, 2023), available at https://arxiv.org/pdf/2201.09035.
[91] *Id.*
[92] *Id.*

comprised of multiple disparate components that can be designed to interact in myriad ways—giving rise to complex questions of whether various regulatory requirements apply at all, and if so to whom.

A few of the key legal frameworks that DeFi projects must consider include: (i) the Commodity Exchange Act and its registration requirements, anti-fraud provisions, anti-manipulative provisions, and commodity pool/commodity trading advisor requirements; (ii) securities laws including the Securities Act, Exchange Act, Investment Company Act, and Investment Advisor Act, including their respective registration and disclosure requirements and market conduct and anti-fraud rules; (iii) the Bank Secrecy Act and State Money Transmission laws and their respective know-your-customer and anti-money laundering requirements; (iv) payments and consumer finance regulation; (v) federal sanctions and anti-terrorism regimes; and (vi) other state licensing requirements such as New York's BitLicense, to name a few.[93] In addition, a spectrum of non-financial laws and regulations such as antitrust, intellectual property, data protection, advertising regulation, and others, must also be closely minded.

When addressing these legal frameworks, a few of the features that separate DeFi from conventional finance warrant particular attention.

Global permissionless networks. Deploying financial applications on global permissionless networks brings to the forefront complications involving the application of laws based on the location or identity of those who use the service, including sanctions regimes, KYC and AML requirements, and others.[94]

Technology Layers and Composability. What a user might perceive as a single DeFi service, is often comprised of multiple distinct technical functions, which may not all be developed, deployed, or managed by the same group (and some of which may not be managed by any group).[95] For example, front-end user interfaces, underlying smart contracts, and third-party custody solutions may each be developed and deployed separately, complicating questions about the allocation of responsibility.[96]

Adding to the technological fragmentation, one of the primary benefits and challenges in DeFi is composability, which refers to the ability to combine various protocols and smart contracts to create new, complex financial products and services.[97]

---

[93] Wright, Aaron, and Gary DeWaal, "The Growth and Regulatory Challenges of Decentralized Finance," *TAC Virtual Currency Subcommittee* 38-39 (Dec. 14, 2020), available at https://www.cftc.gov/media/5471/TAC121420_GrowthRegulatoryChallengesDecentralizedFinance/download.

[94] Redbord, Ari, "Crypto Regulation: U.S. Treasury Statement on DeFi Emphasizes Anti-Money Laundering Rules," *Forbes Digital Assets* (Apr. 7, 2023), available at Crypto Regulation: U.S. Treasury Statement On DeFi Emphasizes Anti-Money Laundering Rules (forbes.com).

[95] Schar, Fabian, "DeCentralized Finance: On Block- and Smart Contract-Based Financial Markets" 169 (2Q 2021).

[96] *See Id. at* 171 (discussing dependencies).

[97] *Id. at* 168-169.

Composability enables innovation and efficiency, but it also introduces legal complexities concerning liability, transparency, and accountability.[98]

Moreover, the source code for most DeFi applications is publicly available. This fact, coupled with a technology stack that is decentralized, fragmented, and composable, makes it particularly hard to enforce legal limits in practice. If any single component is shut down in one jurisdiction, a nearly identical function (or several) could pop up anywhere in the world to take its place, with little incremental cost or expertise required.

Nature of the assets. Crypto assets in DeFi may include securities, commodities, derivatives, or other complex financial assets, which has significant implications for their treatment under U.S. laws.

Governance also introduces a unique dimension to the legal landscape. The legal status and responsibilities of governance token holders remains unclear, particularly with respect to theories that would seek to hold governance token holders jointly and severally liable for the conduct of a DAO.[99]

Cybersecurity. DeFi projects must address the issue of smart contract security.[100] The high-profile incidents of smart contract exploits and hacks have underscored the importance of rigorous security auditing and testing.

With these considerations in mind, the remainder of this Chapter provides an overview of key legal regimes, enforcement actions, and private litigation impacting DeFi.

1. OFAC (Sanctions)

The Department of Treasury's Office of Foreign Assets Control (OFAC) administers sanctions, monitors compliance with these sanctions, and conducts civil investigations into apparent violations of sanctions regulations.[101] OFAC has recognized that digital assets can be used by individuals and entities who seek to violate or evade U.S. sanctions.[102]

Since 2018, OFAC has been active in the digital assets area, imposing sanctions on perpetrators of ransomware attacks, who often make ransom demands in

---

[98] *See Id. at* 171.

[99] Makarov, Igor & Antoinette Schoar, *Brookings Papers on Economic Activity*, "Cryptocurrencies and Decentralized Finance (DeFi)" 35 (Mar. 24, 2022), available at https://www.brookings.edu/wp-content/uploads/2022/03/SP22_BPEA_MakarovSchoar_conf-draft.pdf; Wharton Blockchain and Digital Asset Project & World Economic Forum, *DeFi Beyond the Hype—The Emerging World of Decentralized Finance* 6 (May 2021).

[100] OECD, "Why Decentralized Finance (DeFi) Matters and the Policy Implications" 34 (2022), available at https://www.oecd.org/daf/fin/financial-markets/Why-Decentralised-Finance-DeFi-Matters-and-the-Policy-Implications.pdf.

[101] OFAC, "About OFAC," available at https://ofac.treasury.gov/about-ofac.

[102] Office of Foreign Assets Control, Sanctions Compliance Guidance for the Virtual Currency Industry (Oct. 2021), available at https://ofac.treasury.gov/media/913571/download?inline.

cryptocurrency; entities that facilitate the digital ransom payments; and more recently, "nested" cryptocurrency exchanges, a darknet market, and mixers that were used by a variety of illicit actors.[103]

In 2021, OFAC published sanctions compliance guidance for the virtual currency industry.[104] OFAC's sanctions compliance guidance for the virtual currency industry emphasizes the importance of compliance with U.S. economic and trade sanctions, particularly for businesses operating in the virtual currency space. The guidance outlines the potential risks associated with engaging in transactions involving virtual currencies that may violate OFAC sanctions. Key points from the guidance include:

- Risk Assessment and Due Diligence[105]: Virtual currency businesses are advised to conduct comprehensive risk assessments and due diligence on their customers and transactions to identify potential sanctions risks. This includes verifying the identities of customers and counterparties and monitoring their activities for any links to sanctioned individuals or entities.
- Transaction Screening[106]: Businesses in the virtual currency industry should implement robust screening mechanisms to ensure that transactions do not involve sanctioned individuals or entities. This may involve using screening software or adopting risk-based approaches to identify and address high-risk transactions.
- Blocking and Reporting[107]: If a virtual currency business identifies a transaction that may be in violation of OFAC sanctions, it is required to block the transaction and promptly report it to OFAC. Failure to do so may result in penalties and enforcement actions.
- Sanctions Compliance Program[108]: OFAC recommends that virtual currency businesses establish and maintain a formal sanctions compliance program to ensure ongoing compliance with sanctions regulations. This includes appointing a designated compliance officer and providing regular training to employees on sanctions-related matters.
- Voluntary Self-Disclosure[109]: Virtual currency businesses that discover potential violations of OFAC sanctions are encouraged to voluntarily self-disclose such

---

[103] *See, e.g.*, OFAC, "Treasury Designates Iran-Based Financial Facilitators of Malicious Cyber Activity and for the First Time Identifies Associated Digital Currency Addresses," Press Release (Nov. 28, 2018), available at https://home.treasury.gov/news/press-releases/sm556.
[104] Office of Foreign Assets Control, Sanctions Compliance Guidance for the Virtual Currency Industry (Oct. 2021), available at https://ofac.treasury.gov/media/913571/download?inline.
[105] *Id.*
[106] *Id.*
[107] *Id.*
[108] *Id.*
[109] *Id.*

violations to OFAC. Self-disclosure may be considered a mitigating factor in determining enforcement actions.

- Third-Party Service Providers[110]: Virtual currency businesses are reminded to exercise caution when engaging with third-party service providers, such as wallet providers or exchanges, to ensure that they also comply with OFAC sanctions.
- Emerging Risks and Technologies[111]: OFAC acknowledges that the virtual currency industry is constantly evolving, and businesses should be vigilant in assessing emerging risks and new technologies that may pose sanctions compliance challenges.

Sanctions compliance has become a lighting-rod issue for DeFi. In May 2022, OFAC issued sanctions for the first time against a virtual currency mixer, Blender.io, which the DPRK used to support its malicious cyber activities associated with money laundering.[112] Approximately six weeks before OFAC's actions, Lazarus group, the DPRK state-sponsored cyber hacking group, carried out the largest virtual currency heist to date—worth almost $620 million at the time—from a blockchain project linked to the online game Axie Infinity.[113] Blender.io, a mixer that obfuscates transactions on the Bitcoin blockchain, was used in processing more than $20.5 million of the illicit proceeds.[114]

And in August 2022, OFAC issued sanctions against an additional virtual currency mixer, Tornado Cash, which had been used to launder more than $7 billion worth of virtual currency since its creation in 2019, including over $455 million stolen by the Lazarus Group.[115] If current trends continue, it's clear that sanctions compliance issues will continue to be of paramount importance to projects building in the DeFi space.

The Tornado Cash Case. Tornado Cash was a prominent mixer on the Ethereum blockchain, enabling users to obfuscate the connection between a sender of crypto and the recipient.[116] OFAC concluded that malicious actors exploited this privacy feature to engage in illicit activities, including money laundering and sanctions evasion, and as a

---

[110] *Id.*
[111] *Id.*
[112] U.S. Dep't of Treasury, "U.S. Treasury Issues First-Ever Sanctions on a Virtual Currency Mixer, Targets DPRK Cyber Threats," Press Release (May 6, 2022), available at https://home.treasury.gov/news/press-releases/jy0768.
[113] *Id.*
[114] *Id.*
[115] U.S. Dep't of Treasury, "U.S. Treasury Sanctions Notorious Virtual Currency Mixer Tornado Cash," Press Release (Aug. 8, 2022), available at https://home.treasury.gov/news/press-releases/jy0916.
[116] Nadler, Matthias & Fabian Schar, "Tornado Cash and Blockchain Privacy: A Primer for Economists and Policymakers," Federal Reserve Bank of St. Louis Review 123 (2Q 2023), available at https://research.stlouisfed.org/publications/review/2023/02/03/tornado-cash-and-blockchain-privacy-a-primer-for-economists-and-policymakers.

result it placed the smart contract addresses comprising the Tornado Cash protocol on the sanctions list.[117]

This was a notable development because sanctions law contemplates imposing sanctions on foreign persons or entities, not technology, and the technology at issue here (the Tornado Cash protocol), had substantial legitimate use cases by American citizens in addition to illegitimate uses for foreign persons and entities.[118] Litigation ensued, with users of Tornado Cash challenging OFAC's authority to impose sanctions on a smart contract.[119]

The Department of the Treasury has presented several arguments supporting the imposition of sanctions on the Tornado Cash protocol[120]:

- National Security Concerns: OFAC contends that the use of privacy-focused DeFi protocols like Tornado Cash poses a significant threat to national security. These protocols may enable malicious actors to move funds undetected and finance illicit activities, undermining the United States' efforts to combat terrorism and other threats.
- Deterrence: Imposing sanctions on DeFi protocols allegedly used for illicit purposes serves as a deterrent against potential wrongdoers. It sends a strong message that the U.S. government takes such activities seriously and will take action to disrupt illegal financial activities.
- Enhancing AML/CFT Compliance: Sanctioning Tornado Cash may serve as a catalyst for increased Anti-Money Laundering (AML) and Combating the Financing of Terrorism (CFT) compliance within the DeFi space. It highlights the need for DeFi platforms and users to implement robust AML/CFT measures to prevent misuse of their services.

The civil suit against the Department of the Treasury challenging the imposition of sanctions on Tornado Cash has presented counterarguments[121]:

- DeFi Protocol Neutrality: Critics argue that Tornado Cash, as a decentralized protocol, is neutral and agnostic to the actions of its users. The protocol itself does not engage in any illicit activities, and its code operates on a trustless and automated basis.
- Privacy as a Fundamental Right: The civil suit raises the issue of privacy as a fundamental right. Privacy-focused DeFi protocols, like Tornado Cash, offer

---

[117] U.S. Dep't of Treasury, "U.S. Treasury Sanctions Notorious Virtual Currency Mixer Tornado Cash," Press Release (Aug. 8, 2022), available at https://home.treasury.gov/news/press-releases/jy0916.
[118] *See* OFAC FAQ No. 1095, available at https://ofac.treasury.gov/faqs/1095.
[119] Complaint, *Coin Center v. Yellen*, Case No. 22-cv-20375 (N.D. Fl.).
[120] U.S. Dep't of Treasury, "U.S. Treasury Sanctions Notorious Virtual Currency Mixer Tornado Cash," Press Release (Aug. 8, 2022), available at https://home.treasury.gov/news/press-releases/jy0916.
[121] Complaint, *Coin Center v. Yellen*, Case No. 22-cv-20375 (N.D. Fl.).

users the ability to protect their financial information and transactions from surveillance. Banning such protocols might infringe upon individuals' right to financial privacy.

- Ineffectiveness of Sanctions: Critics question the effectiveness of imposing sanctions on DeFi protocols. They argue that bad actors can easily switch to other privacy-focused protocols or develop new methods to evade detection, making the sanctions less impactful in curbing illicit activities.

The Tornado Cash case exemplifies the collision between decentralized finance and traditional regulatory frameworks. As the DeFi space continues to evolve, policymakers, regulators, and legal professionals face the challenge of striking a balance between financial privacy and national security concerns. Addressing the issue of OFAC sanctions in the DeFi context requires nuanced consideration of the technology's unique characteristics and its potential implications for global financial systems. The outcome of the Tornado Cash case may have significant implications for the future regulation of DeFi and how privacy-focused protocols are treated within the broader legal framework of sanctions and financial regulation.

2. BSA, State Money Transmitter (KYC/AML)

The decentralized nature of DeFi platforms poses unique challenges for regulatory compliance, particularly in areas such as the Bank Secrecy Act (BSA) and state money transmitter laws, and their respective Know Your Customer (KYC) and Anti-Money Laundering (AML) requirements. KYC and AML regulations are fundamental components of financial crime prevention. They require financial institutions, including DeFi platforms, to verify the identities of their customers, conduct ongoing monitoring for suspicious activities, and report any suspicious transactions to authorities.

Bank Secrecy Act (BSA). The BSA is a key federal law that requires financial institutions, including money services businesses (MSBs), to establish and implement anti-money laundering programs to detect and prevent illicit financial activities. In the context of DeFi, decentralized platforms and protocols may qualify as MSBs, depending on their activities and the types of services they offer. The BSA imposes obligations on these entities to register with FinCEN, file Currency Transaction Reports (CTRs) and Suspicious Activity Reports (SARs), and maintain robust AML procedures.

FinCEN, the government agency charged with administering the BSA, released a Risk Assessment on DeFi in 2023.[122] The assessment identifies potential vulnerabilities in DeFi platforms, including the anonymity of users, cross-border transactions, and the use of privacy-enhancing technologies.[123] It emphasizes the need for DeFi platforms to

[122] U.S. Dep't of Treasury, "Illicit Finance Risk Assessment of Decentralized Finance" (Apr. 2023), available at https://home.treasury.gov/system/files/136/DeFi-Risk-Full-Review.pdf.
[123] *Id.*

adopt effective risk-based AML programs to address these challenges and protect the integrity of the financial system.[124]

State Money Transmitter Laws. State money transmitter laws vary from state to state and can apply to certain activities within the DeFi ecosystem. These laws typically require entities engaged in the transmission of virtual currencies or funds to obtain a money transmitter license from each state in which they operate, and to adhere to a variety of ongoing requirements including KYC and AML obligations, among others.

3. SEC Enforcement

While public SEC enforcement actions have primarily focused on token sellers and promoters,[125] and more recently centralized trading platforms,[126] the SEC has brought at least one enforcement action against a purported DeFi protocol. In November 2018, the SEC announced that it had settled charges against EtherDelta's creator, Zachary Coburn.[127] The SEC alleged that EtherDelta provided a platform for users to trade digital assets that were considered securities under federal securities laws.[128] According to the SEC's press release, EtherDelta was facilitating the buying and selling of tokens that met the definition of securities without registering as a national securities exchange or operating under an exemption.[129] The SEC argued that decentralized exchanges like EtherDelta must comply with federal securities laws and registration requirements.[130] The settlement with Coburn required him to pay over $300,000 in disgorgement, interest, and penalties, and to refrain from any further securities trading activities.[131]

More recently, Uniswap Labs has reportedly been the subject of an investigation by the SEC for years.[132] Sushiswap has similarly been the subject of investigation, with its

---

[124] U.S. Dep't of Treasury, "Illicit Finance Risk Assessment of Decentralized Finance" (Apr. 2023), available at https://home.treasury.gov/system/files/136/DeFi-Risk-Full-Review.pdf.
[125] *See* U.S. SEC, Crypto Assets and Cyber Enforcement Actions, available at https://www.sec.gov/spotlight/cybersecurity-enforcement-actions.
[126] *See, e.g.*, SEC, "SEC Charges Coinbase for Operating as an Unregistered Securities Exchange Broker, and Clearing Agency," Press Release No. 2023-102 (June 6, 2023), available at https://www.sec.gov/news/press-release/2023-102; SEC, "SEC Files 13 Charges Against Binance Entities and Founder Changpeng Zhao," Press Release No. 2023-101 (June 5, 2023), available at https://www.sec.gov/news/press-release/2023-101; SEC, "SEC Charges Crypto Asset Trading Platform Bittrex and its Former CEO for Operating an Unregistered Exchange, Broker, and Clearing Agency," Press Release No. 2023-78 (April 17, 2023), available at https://www.sec.gov/news/press-release/2023-78.
[127] SEC, "SEC Charges EtherDelta Founder with Operating an Unregistered Exchange," Press Release No. 2018-258 (Nov. 8, 2018), available at https://www.sec.gov/news/press-release/2018-258.
[128] *Id.*
[129] *Id.*
[130] *Id.*
[131] *Id.*
[132] Michaels, Dave and Alexander Osipovich, "Regulators Investigate Crypto-Exchange Developer Uniswap Labs," *The Wall Street Journal* (Sep. 3, 2021), available at

CEO openly discussing receipt of a subpoena in 2023.[133] As a result, and potentially depending on the progress of its cases against centralized exchanges, it is possible that further actions against DeFi protocols may be on the horizon.

4. CFTC Enforcement

The CFTC has also been active in the DeFi space, most notably including its 2022 enforcement action against bZeroX, LLC and its founders, and subsequent litigation against Ooki DAO.[134] The CFTC alleged that bZeroX operated an unregistered derivatives platform and engaged in other violations of commodities trading regulations, which it then transitioned to purported decentralized governance, in the form of Ooki DAO, to evade regulation.[135]

After settling with bZeroX and the founders,[136] the CFTC brought litigation against OokiDAO for the ongoing operation of the protocol.[137] The court found Ooki DAO liable, accepting a theory that the DAO operated as an unincorporated association in which all token holders are jointly and severally liable.[138] The lawsuit's outcome could have important implications for other DeFi projects similarly structured as DAOs.

5. Private Litigation

There are also several ongoing purported class actions against DeFi protocols and/or their founders, investors, and other entities that allegedly support their operation, including cases concerning PoolTogether, Compound, and Bancor, among others.

PoolTogether. In the lawsuit against PoolTogether, the plaintiff argued that the DeFi protocol's savings product constituted an illegal lottery in violation of New York state law.[139] The plaintiffs contended that PoolTogether's mechanism, where users deposited funds with the into a "liquidity pool" for various investments, forgoing a

---

https://www.wsj.com/articles/regulators-investigate-crypto-exchange-developer-uniswap-labs-11630666800.

[133] Grey, Jared, "Head Chef Jared Grey's Official SEC Statement and FAQ," Sushi Forum (Apr. 7, 2023), available at https://forum.sushi.com/t/head-chef-jared-greys-official-sec-statement-faq/11918.

[134] "CFTC Imposes $250,000 Penalty Against bZeroX, LLC and Its Founders and Charges Successor Ooki DAO for Offering Illegal, Off-Exchange Digital Asset Trading, Registration Violations, and Failing to Comply with Bank Secrecy Act," CFTC Release No. 8590-22 (Sep. 22, 2022), available at https://www.cftc.gov/PressRoom/PressReleases/8590-22.

[135] *Id.*

[136] *Id.*

[137] *CFTC v. Ooki DAO*, Case No. 22-cv-5416 (N.D. Ca.).

[138] Order Granting Motion for Default Judgment, *CFTC v. Ooki DAO*, Case No. 22-cv-5416 (N.D. Ca.); Corso, Jessica, "CFTC Hails Novel Ruling to Shutter Ooki DAO Crypto Site," *Law360* (June 9, 2023).

[139] Complaint ¶¶ 116-19 (Oct. 29, 2021), *Kent v. Pooltogether, Inc.*, Case No. 21-cv-6025 (E.D.N.Y.).

guaranteed interest rate in exchange for a chance at a greater return, to a lottery.[140] The court dismissed the lawsuit without directly addressing whether PoolTogether's savings product qualified as a lotter, finding that the plaintiff had failed to allege a concrete injury and standing to bring the case.[141]

bZx DAO. Following the enforcement action by the CFTC, a private class action was filed seeking to hold liable founders of the bZx protocol and two early investors, on the theory that they were all jointly and severally liable as partners in a purported partnership by virtue of holding governance tokens, for plaintiffs' losses allegedly sustained in a hack of the protocol.[142] The theory survived a motion to dismiss and remains pending.[143]

Compound. The lawsuit concerning Compound alleges violations of federal securities laws in connection with the unregistered issuance and sale of the governance token COMP, which plaintiffs' claim was a security.[144] The plaintiffs sued the DAO, along with its developers, and certain investors, who they assert are jointly and severally liable as partners by virtue of holding the COMP governance token.[145] The case is before the same judge who accepted a similar joint liability theory in the CFTC's Ooki DAO litigation, discussed above.

Bancor. A purported class action filed against Bancor DAO and various persons and an entity affiliated with the Bancor protocol, is notable because it alleges, among other things, that contributions to Bancor's AMM and receipt of LP tokens constituted an unregistered securities offering by defendants, and also that defendants operated as unlicensed brokers and dealers with respect to the "Bancor exchange."[146]

Most of the cases set forth above remain pending and none has yet resulted in a precedential decision on a core issue, but the cases are notable because they confirm an appreciable risk to DeFi protocols in the form of private litigation, and also suggest that the future evolution of the law may not be shaped only by legislators and enforcement actions, but also by the decentralized market forces of private litigation.

---

[140] Memorandum and Order 3-4 (June 7, 2023), *Kent v. Pooltogether, Inc.*, Case No. 21-cv-6025 (E.D.N.Y.).
[141] Memorandum and Order 15-16 (June 7, 2023), *Kent v. Pooltogether, Inc.*, Case No. 21-cv-6025 (E.D.N.Y.); Perera, Katryna, "Court Tosses Suit Alleging DeFi Protocol Ran Illegal Lottery," *Law360* (June 7, 2023), available at https://www.law360.com/articles/1686439/court-tosses-suit-alleging-defi-protocol-ran-illegal-lottery.
[142] Complaint ¶¶ 1-2, *Sarcuni v. bZx DAO*, Case No. 22 CV 0618 (S.D. Ca.); Ruscoe, Emily, "Crypto Investors Sue Over $55M Theft in Phishing Scam," *Law360* (May 3, 2022), available at https://www.law360.com/articles/1489573/crypto-investors-sue-over-55m-theft-in-phishing-scam.
[143] Order 29 (Mar. 27, 2023), *Sarcuni v.* bZx *DAO*, Case No. 22 CV 0618 (S.D. Ca.).
[144] Complaint ¶¶ 4-6 (Dec. 8, 2022), *Houghton v. Compound DAO*, Case No. 22-cv-7781 (N.D. Ca.).
[145] *Id. at* ¶¶ 105-11.
[146] Complaint ¶¶ 4-11 (May 11, 2023), *Basic v. BProtocol Foundation*, Case No. 23-cv-00533 (W.D. Tx.)

E. Conclusion

The DeFi space presents a landscape rich in novelty and innovation, but also complexity. It cuts across a multitude of regulatory regimes and implicates many different legal issues. Agencies like OFAC, the BSA, SEC and CFTC all have potential jurisdictional claims in this arena, each emphasizing distinct aspects of compliance, from securities laws to sanctions to anti-money laundering requirements. Additionally, private litigation has also come into the forefront with a slew of class action lawsuits being filed against DeFi protocols the last few years. With the growing prominence of DeFi and crypto generally in the United States and globally, it is likely that regulators and private litigants will continue adding to the myriad of legal complexities and projects and protocols will need to act accordingly to get ahead of these issues for DeFi to flourish.

Raising Capital

Patrick Daugherty*

A. Introduction

Software protocols and applications may be, or become, decentralized, but they don't begin that way. They are incubated and hatched by live human beings conducting business. Therefore, and especially in the early days, the inventors and developers of permissionless blockchain protocols and applications have the same needs that all early-stage businesses have. These needs include organization, governance and financing.

Those topics will be discussed in this chapter, beginning with organization (which includes governance), then dwelling at length upon financing, which proceeds in stages. Early financing rounds are structured in the digital asset industry the same way they are structured in the broader technology and financial services industries—as transactions exempt from Securities Act registration by reason of reliance on one or more exemptions. The business is initially organized as a corporation or limited liability company under U.S. law but might instead be organized in a non-U.S. jurisdiction. The business will likely migrate offshore so as to lawfully avoid U.S. regulation as much as possible, in that U.S. financial services regulation is decidedly hostile at present to the development and use of permissionless blockchain technology.

The use of available registration exemptions will be explained. SEC Regulation S will be explored in depth because it is the optimal vehicle for capital raising, under current law, beyond earliest-stage "angel" and venture capital financing. In doing so,

---

* Daugherty is a Partner and founder of the digital assets practice of Foley & Lardner LLP. Based in Chicago, he also is a member of the Bars of New York and Washington, D.C., and teaches a seminar on digital assets at Cornell Law School. As an SEC Executive Staff lawyer in 1989, he assisted the late Linda C. Quinn, Director of the Division of Corporation Finance, in the formulation of Regulation S, discussed at length in this chapter. Mr. Daugherty thanks Richard Spencer, a partner of Campbells based in Grand Cayman, for assistance with Section 7 of this chapter, and J.P. Riley, a Foley summer associate, for footnoting help. Helpful comments were received from Kimberly A. Prior, Miami partner of Winston & Strawn LLP, and participants in the January 2023 conference on digital assets sponsored by the University of Chicago Law School Center for Law and Finance. The concept of this chapter was suggested by Joshua Ashley Klayman Kuzar, senior counsel at Linklaters in New York. Any errors that remain are the author's alone. Kimberly Prior reviewed this chapter.

this chapter will explain how Regulation S can be used and will identify interpretive issues and risks and how best to address them. The content of disclosure prepared to satisfy antifraud mandates is also an important topic. It is treated in this chapter in so far as pending legislation relating to mandatory disclosure for token offerings is described and recommended as guidance.

There are many topics related to raising capital that are beyond the scope of this chapter. These include anti-money-laundering ("AML"), know-your-customer ("KYC") and sanctions compliance, which is treated only in passing. Also, the regulation of brokers, dealers, exchanges and clearing agencies is at issue in cases brought by the SEC against Coinbase and Kraken, among other centralized crypto platforms. This chapter does not address those topics, either.

The focus of this chapter is on lawful compliance with Securities Act registration exemption requirements in capital raising transactions by blockchain technology development teams.

B. Introduction

In advising a development team, it is essential to begin with the end in mind. It is unhelpful to begin well yet end with an enterprise that cannot operate lawfully. The end is not reached when a business is duly organized under some body of law, but rather when the team's ambition to create a self-sustaining blockchain-based ecosystem has come to fruition. Legal advice and drafting skill is needed from conception of the protocol through all stages of financing and technology development and deployment until a decentralized autonomous organization (or "DAO") is operating or the protocol is fully functional, or both. Compliance with applicable law is needed on each step of the journey.

Laws to consider and apply when advising a blockchain technology development team include business organization law, securities law, the Commodity Exchange Act of 1936 and related rules and regulations (the "CEA"), money transmission law, banking law, tax law, consumer protection law, commercial law and intellectual property law. All of these laws, and others, should inform the advice and drafting approaches of lawyers advising clients with respect to protocol and token development and launch.

One should assume that, at least in its early stages, the protocol and token will be correctly classified as a "security" under applicable law. This is the highly likely outcome when applying the *Howey*[1] analysis reflected in "When Howey Met Gary (Plastic)"[2] and the FinHub Framework.[3] It is also supported by significant, recent case

[1] SEC v. W.J. Howey Co., 328 U.S. 293 (1946).

[2] William Hinman, *Digital Asset Transaction: When* Howey *Met* Gary (Plastic), U.S. SEC. & EXCH. COMM'N (June 14, 2018), https://www.sec.gov/news/speech/speech-hinman-061418.

[3] *Framework for "Investment Contract" Analysis of Digital Assets*, U.S. SEC. & EXCH. COMM'N (last modified Mar. 8, 2023), https://www.sec.gov/corpfin/framework-investment-contract-analysis-digital-assets (the

law. For example, in *Ripple Labs*,[4] Judge Torres of the Southern District of New York held that sales of the XRP token by Ripple Labs directly to institutional investors in negotiated transactions documented by definitive agreements were a securities offering under *Howey*.[5]

Because the protocol and token, at least in early stages, will be an investment contract, and therefore a security, every offer and sale of the token must comply with Section 5 of the Securities Act, which means that every offer and every sale must be either registered or exempt.[6] "Must" is the correct word in this context because the consequences of making unregistered, non-exempt offers or sales can be severe. They can include rescission, civil liability, money penalties, administrative sanctions and, in a particularly extreme case, criminal liability. For this reason, clients are advised—to focus their attention—that every offer and sale of a security is either (1) registered or (2) exempt or (3) unlawful. Under current law, token sales are almost never registered because the SEC has chosen to make it extremely difficult to do so. Since unlawful behavior is necessarily avoided, care must be taken to assure the availability of an exemption from Securities Act registration.

This chapter will mainly discuss exempt transactions for digital assets. Three exemptions are useful: Regulation S; Rule 701; and the exemption (or cluster of exemptions) commonly referred to as the "private offering" exemption. Registered transactions are not discussed much because, to date, there have been few, and fundamentally they have failed, because the registration requirements for securities issued by traditional businesses do not fit blockchain-enabled protocols, especially decentralized protocols (which have no central management). Appropriate digital asset disclosure also will be discussed in this chapter.

"FinHub Framework"). A significant *Howey* interpretation issued and oft-cited by the SEC itself (rather than the SEC Staff or the courts) is Report of Investigation Pursuant to Section 21(a) of the Securities Exchange Act of 1934: The DAO, SEC Release No. 81207 (July 25, 2017), https://www.sec.gov/litigation/investreport/34-81207.pdf.

[4] SEC v. Ripple Labs, Inc., Case No. 20 Civ. 10832 (S.D.N.Y. July 13, 2023), *available at* https://www.crypto-law.us/wp-content/uploads/2023/07/2023.07.13-Order.pdf, *motion for certification of interlocutory appeal denied by order dated Oct. 3, 2023*, https://casetext.com/case/sec-exch-commn-v-ripple-labs-28.

[5] *See* SEC v. Ripple Labs, Inc., *supra* note 4 (S.D.N.Y. July 13, 2023), at 16-22.

[6] 15 U.S.C. § 77e(a) ("Unless a registration statement is in effect as to a security, it shall be unlawful for any person directly or indirectly—(1) to make use of any means or instruments of transportation or communication in interstate commerce or of the mails to sell such security through the use or medium of any prospectus or otherwise; or (2) to carry or cause to be carried through the mails or in interstate commerce, by any means or instruments of transportation, any such security for the purpose of sale or for delivery after sale."); *Id.* § 77e(c) ("It shall be unlawful for any person, directly or indirectly, to make use of any means or instruments of transportation or communication in interstate commerce or of the mails to offer to sell or offer to buy through the use or medium of any prospectus or otherwise any security, unless a registration statement has been filed as to such security . . . .").

C. Business Organization

Before a protocol can emit tokens, the protocol needs to be invented. Live human beings are currently required for that. They will organize themselves as some sort of enterprise. They will have roles in an entity. Because the protocol and tokens will be securities, at least initially, the usual path, if they are to be offered publicly, is to offer them outside the United States. The domicile of the entity organized at the inception of the project may be either within the United States or outside the United States. If it's on-shore, that entity will later migrate off-shore, as explained below.

Typically, a laboratory (or "Lab") is organized under U.S. law. Two examples are Ava Labs and Solana Labs. The Lab is essentially a research-and-development operation. The founders of the Lab may include blockchain technology scientists and engineers and other talented individuals with skill sets necessary for any technology start-up venture. The founders and earliest investors typically receive equity in the Lab in exchange for their contributions of talent and money.

The Lab might be organized as a corporation or as a limited liability company (an "LLC"). The choice tends to be driven by the expectations of prospective investors. Venture capitalists prefer to invest in "C" corporations (rather than "S" corporations or LLCs), so the usual decision is to organize the Lab as a C corporation. In the discussion that follows, the reader should assume that the Lab has been organized as a Delaware "C" corporation whose equity is issued initially to the founders.

The business of the Lab will be to develop and execute a plan to create a protocol, its native token and a thriving ecosystem with online and real-world use. This is mainly about software coding and is driven by computer scientists and engineers, but it also involves commercial contracts among ecosystem participants. For example, bank accounts need to be established in order to pay bills requiring payment in U.S. dollars. Office space and off-the-shelf software need to be leased. Administrative staff need to be hired and pa*id.*

Upon and after organization, the Lab will raise equity capital through private offerings. It also may incentivize managers and service providers with equity grants or token grants (or both) under SEC Rule 701 (which is discussed in Section G of this chapter). As these financings and arrangements are made, Lab personnel continue their business of inventing the protocol and designing a token or tokens.

At some point, a non-U.S. entity will be organized by persons in or associated with the Lab. In order to orient its activities toward the ecosystem rather than equity owners or managers (what the FinHub Framework calls "Active Participants" (APs)[7]), the best choice for that non-U.S. entity will be a foundation that by design has no shareholders.

---

[7] *See Framework for "Investment Contract"* Analysis *of Digital Assets*, *supra* note 3 (defining an "Active Participant" or "AP" as a "promoter, sponsor, or other third party (or affiliated group of third parties)" who "provides essential managerial efforts that affect the success of the enterprise, and investors reasonably expect to derive profit from those efforts").

Examples of this structure are found in the laws of Switzerland[8] and the Cayman Islands.[9] A shareholder-less foundation is the best choice for the non-U.S. entity because such a foundation is responsible for its beneficiaries, who are participants in the ecosystem, bit for no one else. Specifically, it is not responsible for or accountable to its shareholders, as it has none.[10]

Early-stage organization and capital raising by the Lab will be essentially the same as for most technology industry ventures. The similarities to other kinds of start-ups include:

- choice of domicile and the "LLC vs. 'S' corporation vs. 'C' corporation" decision, noted *infra*;
- the preparation of organizational documents (such as an operating agreement or a charter and bylaws and shareholders' agreement) differentiating the rights and duties of equity holders versus the rights and duties of the board of directors or other board, and versus the rights and duties of managers (who may, but need not, be equity holders or board members, or both);
- a "seed" round of equity financing (which may be "angel" financing);
- a "Series A round," typically targeting venture capitalists; then
- later, a "Series B" round and possibly other rounds.

There is an active venture capital community and angel investment in the digital assets industry. Prominent Northern California firms with significant digital assets industry investments include Sequoia Capital, Andreessen Horowitz (known as "A16z"), Pantera Capital, Coinbase Ventures, Polychain Capital, Dragonfly Capital and Lightspeed Ventura Partners, among others. Digital Currency Group ("DCG") and Galaxy Digital in New York also are significant. Significant venture investors in digital assets based outside the United States include NGC Ventures (Singapore), LD Capital (Beijing), Fenbushi Capital (Shanghai) and Binance Labs (Hong Kong).

Prominent angel investors in the industry include Naval Ravikant (co-founder of AngelList) Roger Ver (known as "Bitcoin Jesus") and Barry Silbert (founder and owner of DCG), among many others. Many early winners in the evolution of this industry have become angel investors.

---

[8] *See* SCHWEIZERISCHES Zivilgesetzbuch [ZGB], CODE CIVIL [CC], CODICE CIVILE [CC] [CIVIL CODE] Dec. 10, 1907, SR 2210, RS 210, art. 80–89 (Switz.) (stating the laws surrounding the formation of foundations).

[9] *See* foundation Companies Law, (2017) EXTRAORDINARY GAZETTE (Cayman Is.).

[10] *See infra* note 86 and accompanying text.

D. Early Financing Rounds

In the Lab's early rounds of financing, Securities Act private offering requirements must be satisfied, which means compliant use of either the statutory private offering exemption or Regulation D. Also, always, fraud must be avoided, regardless of the exemption that is used. Typically, antifraud compliance is best satisfied by preparation and use of a formal disclosure document.

The key requirements of the statutory private offering exemption are that the offerees be "rich and smart";[11] that "general solicitation" be avoided;[12] that the offerees be relatively few in number;[13] and that the offered securities be purchased "for investment" (which requires a holding period).[14] No particular contents of the disclosure document are mandated.[15]

Three options exist under SEC Regulation D for the offering and sale of securities (including tokens that are or may be securities). Rule 506(c) imposes the fewest restrictions: General solicitation is permitted,[16] and no particular disclosures are required.[17] But only accredited investors can invest in a Rule 506(c) offering,[18] and accredited investor status must be verified for each investor.[19]

"Verification" is not especially challenging, but it does require more than "check-the-box" self-certification by the prospective investor. Review of recent tax returns or employment data generally will suffice.[20] There are companies in the business of

---

[11] *See* SEC v. Ralston Purina Co., 346 U.S. 119, 125 (1953), noting that the applicability of the private offering exemption depends upon "whether the particular class of persons affected need the protection of the Act." In that case, "employees with the duties of artist, bakeshop foreman, clerical assistant," *etc.*, *Id.* at 121, were held to lack the financial sophistication (the relevant "smartness") and risk-bearing capacity ("riches") that justify application of the private offering exemption.

[12] *See* Patrick Daugherty, *Rethinking the Ban on General Solicitation*, 38 EMORY L.J. 67, 91–93 (1989) (discussing the guidance from the SEC Staff regarding the issues arising from general solicitation).

[13] Committee on Federal Regulation of Securities, *Current Issues and Developments in the Duties and Liabilities of Underwriters and Securities Dealers*, 33 THE BUS. LAW. 335, 388 (1977) ("The investment banker will send this abbreviated form of investment circular to a relatively small number of sophisticated institutional offerees in the process of distribution of those securities.").

[14] *Id.* at 340 ("[A] selling concession is not properly earned by a participant in the distribution of securities if those shares are not effectively placed for investment . . . .").

[15] *See Id.* at 336.

[16] *See* 17 C.F.R. § 230.506(c) (providing the conditions under which offerings are not subject to limitation on the manner of the offering).

[17] *See Id.* (enumerating no required disclosures for offerings under paragraph (c) of this section).

[18] *Id.* § 230.506(c)(2)(i) ("All purchases of securities sold in any offering under paragraph (c) of this section are accredited investors.").

[19] *Id.* § 230.506(c)(2)(ii) ("The issuer shall take reasonable steps to verify that purchasers of securities sold in any offering under paragraph (c) of this section are accredited investors.").

[20] *See* Eliminating the Prohibition Against General Solicitation and General Advertising in Rule 506 and Rule 144A Offerings, 78 Fed. Reg. 44771, 44779 (to be codified at 17 C.F.R. pts. 230, 239, 242); *see also SIFMA Guidance on Rule 506(c) Verification*, SIFMA (June 23, 2014), https://www.sifma.org/wp-content/uploads/2017/05/sifma-guidance-on-rule-506c-verification.pdf (providing "guidance to

performing the verification function efficiently. Rule 506(c) is especially useful in making a broad retail solicitation using the internet to identify prospective investors, who can then be curated according to their financial standing. It is used less often for seed, angel or venture capital financing.

Rule 506(b) is the classic private offering safe harbor. Again, no particular contents for a formal disclosure document are mandated as long as the offering is made only to accredited investors.[21] The Lab will want to limit its offering to accredited investors for that very reason, as preparation of the offering memorandum that would be required to include even one unaccredited offeree is time-consuming, expensive and even hazardous as particular line item disclosure requirements might be overlooked. Rule 506(b) is the usual path to follow if the Lab knows everyone, or virtually everyone, that is likely to invest in the round and if the number of such investors is higher than the handful or so that would normally invest using the statutory private offering exemption. It might also or instead be used where the statutory exemption is appropriate but where the Lab r investors prefer the additional comfort associated with use of a safe harbor.

Rule 504 is rarely used but is mentioned nonetheless for the sake of completion. Using Rule 504, the Lab can offer to the general public,[22] but in doing so will be subject to state blue sky laws that are pre-empted for Rule 506 offerings but not for these offerings.[23] Experienced practitioners and their clients avoid blue sky regulation when possible because it can be intrusive and time-consuming and, in any event, imposes compliance burdens that otherwise would be avoided. Rule 504 also allows issuers to generally solicit their securities, does not require disclosure of information to purchasers, and there are no resale restrictions.[24]

Privately offered securities can be resold, but this is best done pursuant to resale safe harbor from Securities Act registration requirements. The applicable safe harbor for a private company security private resale is Rule 144; specifically, Rule 144(b). A holder who is not an affiliate of the issuer at the time of sale and has not been an affiliate for the prior three months ordinarily may resell securities held for at least one year since they were acquired from the issuer or from an affiliate of the issuer.[25] The purchasers in private offerings should expect to covenant to "lock up" the purchased securities by not reselling them until one year has passed and other applicable requirements of Rule 144 have been satisfied.

Securities fraud avoidance is essential in every round of financing, regardless of the particular exemption that is used by the Lab. There is no "exemption" from SEC Rule

---

registered broker-dealers and investment advisers on some verification methods they could use to determine whether certain legal entities qualify as accredited investors).

[21] *See* 17 C.F.R. § 230.506(b).

[22] *See Id.* § 230.504.

[23] Compare *Id.* with *Id.* § 230.506.

[24] *See* 17 C.F.R. § 230.504.

[25] See 17 C.F.R. § 230.144(b)(1)(ii) and § 230.144(d)(1)(ii). Stricter requirements apply to resales by affiliates.

10b-5 or other fraud prohibitions in the securities laws. Fraud is best avoided by crafting written disclosures for delivery to prospective investors within a reasonable time before they make their investment decisions. Preparing disclosure is best done as an iterative process in which Lab personnel prepare segments of information that legal counsel edit, suggesting improvements and additional topics for attention.

Where no particular content of the disclosure is required, as in the case of a statutory private offering, a Rule 506(c) offering or a Rule 506(b) offering to accredited investors only, two models have evolved. One model is a private offering memorandum, covering the business (or proposed business) of the Lab, its actual and anticipated sources and uses of funds, financial statements (if they exist), its management and governance, and most importantly the "risk factors" associated with the Lab and the offering. Unless the business is mature—and it won't be—full details of the business plan will be crucial, as the investor needs to see what steps are expected to occur, and when. The other model avoids creation of a private placement memorandum but includes in the subscription documents the same risk factors (or perhaps a summary of them) that would otherwise be included in the first model.

These models for digital asset Lab private capital raising are generally consistent with the models for other technology-oriented private offerings. The main differences are the need in the former case to explain the protocol, the ecosystem and the token, as these are unique to the digital assets industry, and the risk factors that relate to the Lab and its offering. Well-prepared risk factors for any offering in the digital assets industry are voluminous. This is so regardless of the stage of development of the company.

Examples to consider are the risk factors used in the Coinbase initial public offering[26] and the Robinhood initial public offering.[27] Particularly noteworthy are the headline risks about the infancy of the industry, the extraordinary difficulty in complying with all applicable laws, and the volatility of market prices for digital assets in general. Lawyers who practice in this industry follow risk disclosures in offerings as a matter of course and will adapt the risks disclosed in one offering for client use to the extent applicable. While the risks faced by an exchange or a broker-dealer are not identical to those faced by a Lab, they are close enough that risk disclosures made by the former can be adapted for use by the latter, as appropriate.

The need for thorough disclosure of risks and uncertainties can scarcely be stressed enough. United States securities legislation and regulation is predicated upon full and fair disclosure that is accurate and not misleading. Without it, registration exemption compliance is unavailing, as there will be liability for securities fraud.

---

[26] Coinbase Glob., Inc., Registration Statement (Form S-1) 16–74 (Mar. 23, 2021).
[27] Robinhood Mkts., Inc., Registration Statement (Form S-1) 25–96 (Oct. 8, 2021).

E. Integration

Another essential consideration is lawful "integration" avoidance. Integration, when it applies, causes two (or more) putatively separate offerings to be combined, usually resulting in loss of the registration exemption for one (or all) of them.[28] If the exemption is lost, then Securities Act Section 5 is violated, with the same adverse consequences mentioned earlier in this chapter.[29] Put another way, integration destroys offerings.

There have been two high-profile integration cases in the digital assets industry to date. The first to be decided was *SEC v. Telegram Group Inc.*, decided by Judge Castel of the Southern District of New York.[30] The second was *SEC v. Kik Interactive Inc.*, decided by Judge Hellerstein of the same court.[31] Both cases merit thoughtful consideration in connection with digital assets industry capital raising.

In 2018, Telegram raised $1.7 billion from 175 experienced investors in exchange for a promise to deliver 2.9 billion Gram tokens upon the launch of the Telegram Open Network blockchain. The 2018 offerings used a Simple Agreement for Future Tokens (or "SAFT") structure, in which tokens are not actually delivered until some later date. Telegram characterized these SAFT sales as private offerings. As for the anticipated resales of Grams deliverable under the SAFTs, Telegram viewed them as non-security commodity sales because the Grams, when issued, would not pass the *Howey* test – they would be useful consumptively, would not be supported by Telegram's essential efforts, and would lack a common enterprise. Therefore, in its view, there were two transactions (or sets of transactions), consisting of private offerings of SAFTs followed by non-security commodity resales, none requiring Securities Act registration.[32]

Judge Castel took a different view. He found "as a fact that the economic reality is that the [SAFTs] and the anticipated distribution of Grams by the Initial Purchasers to the public via the TON Blockchain are part of a single scheme."[33] The 2018 SAFT sales were "part of a larger scheme, manifested by Telegram's actions, conduct, statements, and understandings, to offer Grams to the Initial Purchasers with the intent and purpose that these Grams be distributed in a secondary public market, which is the offering of securities under *Howey*."[34]

In reaching this conclusion, the court discounted the standard investment representations made by the Initial Purchasers in the 2018 sales, stating that "legal disclaimers do not control. The representation and warranty that the Initial Purchasers purchased without a view towards resale rings hollow in the face of the economic

---

[28] *See* 17 C.F.R. § 230.152.
[29] *See supra* note 6 and the supporting text.
[30] SEC v. Telegram Grp. Inc., 448 F. Supp. 3d 352 (S.D.N.Y. Mar. 24, 2020) (granting preliminary injunction).
[31] SEC v. Kik Interactive Inc., 492 F. Supp. 3d 169 (S.D.N.Y. Sept. 30, 2020) (granting summary judgment for the government).
[32] *See* Telegram *Grp. Inc.*, 448 F. Supp. 3d at 358.
[33] *Id.* at 367.
[34] *Id.* at 379.

realities." On this view, the 2018 sales were "merely a step in a public distribution of Grams."[35] Because the Initial Purchasers did buy with a view to resale in the court's view, they were statutory underwriters. Further, Telegram had to know that they were statutory underwriters. Therefore, the court ruled that the two sets of transactions were in reality a single "scheme" that was "'a disguised public distribution.'"[36] Because no registration statement had been filed, an injunction blocking the distribution was issued.[37]

Telegram suggests that a SAFT sale is likely to be characterized as a public offering when expectations are high that the underlying tokens will be issued into an environment in which APs continue to control the protocol and build the ecosystem and in which the SAFT purchasers are relying upon APs to perform those functions. The court observed that "an investment of money in a cryptocurrency utilized by members of a decentralized community connected by blockchain technology, which itself is administered by this community of users rather than by a common enterprise, is not likely to be deemed a security . . . ." The court did not find those features present in *Telegram*. On the contrary, it found "an implicit (though formally disclaimed) intention on the part of Telegram to remain committed to the success of the TON Blockchain post-launch."[38] But in another case—in one lacking such a "scheme" because the protocol and token have become sufficiently decentralized or because the ecosystem has become fully functional, with no need for more AP involvement—the result should be different.

Judge Castel's focus in *Telegram* on the "contract, transaction, or scheme" aspect of *Howey* was telling.[39] Observing that the Gram token itself was "little more than alphanumeric cryptographic sequence," he explained:

Howey refers to an investment contract, *i.e.*, a security, as "a contract, transaction or scheme," using the term "scheme" in a descriptive, not a pejorative, sense. This case presents a "scheme" to be evaluated under *Howey* that consists of the full set of contracts, expectations and understandings centered on the sales and distribution of the Gram. *Howey* requires an examination of the entirety of the parties' understandings and expectations.[40]

---

[35] *Id.* at 381.

[36] *Id.* at 380 (quoting SEC v. Cavanagh, 1 F. Supp. 2d 337, 369 (S.D.N.Y. Apr. 20, 1998)).

[37] *Id.* at 382. Judge Castel clarified the scope of his injunction by issuing a subsequent opinion and order applying the injunction to all sales worldwide. *See* SEC v. Telegram Grp. Inc., 19-cv-9439 (PKC), 2020 WL 1547383 (S.D.N.Y. Apr. 1, 2020). He seems to have reached that conclusion mainly because the defendants raised the issue of geographic scope too late. It seems doubtful that he would have reached the same conclusion had *Morrison v. National Australia Bank Ltd.* been briefed earlier. *See* Morrison v. Nat'l Austl. Bank Ltd., 561 U.S. 247 (2010).

[38] Telegram *Grp. Inc.*, 448 F. Supp. 3d at 358.

[39] *See, e.g.*, *Id.* at 367–68 ("'[A] contract, transaction or scheme' is deemed an investment contract if it satisfies the four prongs of the Howey test . . . ." (quoting SEC v. W.J. Howey Co., 328 U.S. 293, 298–99 (1946))).

[40] *Id.* at 379 (citing *Howey*, 328 U.S. at 297–98).

Again, Judge Castel found a "scheme" in *Telegram* that he held to be an investment contract for the purposes of the SEC's motion for a preliminary injunction. He plainly would not have found an investment contract present in a case where there was no such scheme.

Kik is a similar story. Kik envisioned the Kin token as a means of buying and selling digital products and services across different applications, using the Ethereum blockchain. For example, a user might create a song and charge other users Kin to listen to that song. Accumulated Kin could be spent on other applications, such as gaming. In short, Kin were to be used as consumer tokens.

Kin was launched in a putatively private offering (called a "pre-sale") of SAFTs solely to verified accredited investors, followed the day after closing by a token distribution event, or "TDE." But there was nothing private about the TDE. Kik retained, directly and through the Kin foundation (which it controlled), 90% of all issued and outstanding tokens. In addition, no goods or services were available for purchase by Kin holders. So Kin and the ecosystem were not sufficiently decentralized, nor were they fully functional.[41]

Judge Hellerstein ruled that the scheme was an investment contract, discounting (as Judge Castel had done) contractual disclaimers about continuing obligations to Kin purchasers:

This is the nature of a common enterprise, to pool invested proceeds to increase the range of goods and services from which income and profits could be earned or, in the case of Kin, to increase the range of goods and services that holders of Kin would find beneficial to buy and sell with Kin.[42]

He also ruled that Kik cultivated an expectation of profits based on the efforts of others in public statements and at public events promoting Kin, encouraging buyers to hold the token for expected appreciation and disclosing that Kin would be tradable on the secondary market through exchanges.

Judge Hellerstein stated the test for "consumption" versus "investment" as being "whether, under all the circumstances, the scheme was being promoted *primarily* as an investment,"[43] and found for the SEC on that point because of "the essential role of Kik in establishing the market."[44] No consumptive use was available at the time of the distribution.

On the critical question of integration, Judge Hellerstein applied the then-existing five-part test for integration stressing two factors: whether the sales were part of a single plan of financing; and whether the sales were made for the same general purpose. He found that those factors were present, and also found that the same class of securities was involved, classifying SAFTs and the underlying tokens as the same. The author considers that last holding incorrect, but the error does not matter in light of the

---

[41] SEC v. Kik Interactive Inc., 492 F. Supp. 3d 169, 173–75 (S.D.N.Y. Sept. 30, 2020).
[42] *Id.* at 179.
[43] *Id.* (emphasis added) (quoting United States v. Leonard, 529 F.3d 83, 88 (2d Cir. 2008)).
[44] *Id.* at 180.

court's other integration findings. As Judge Hellerstein noted, the putatively private SAFT sales and the public TDE were separated by only one day. In those circumstances, it was correct to integrate the two offerings.

But since then, the law has changed. Both *Telegram* and *Kik* were decided before November 2020, when the SEC adopted Rule 152.[45] Rule 152 covers integration comprehensively. It is not aimed at the digital assets industry, but it does cover the different types of offerings that are discussed in this chapter. Here is how Rule 152 should be applied to these offerings:

- Under the Rule 152(b)(1) safe harbor, an offering made more than 30 days before the start of another offering, or more than 30 days after the termination or completion of another offering, will not be integrated with that offering, unless the first offering to occur is made under a rule permitting general solicitation.46 Therefore, multiple financing rounds can be made without fear of integration so long as none of them is made under Rule 506(c) or another rule that allows general solicitation. This should not present a timing problem even for the fastest-growing Lab and is a significant improvement in the law from a capital raising perspective because, until Rule 152 was adopted, it might have been necessary to wait for as long as six months between rounds.
- Under the Rule 152(b)(2) safe harbor, offers and sales made under Rule 701 or Regulation S, covered infra, are not integrated with other offerings.47 This means that multiple offerings can be conducted concurrently as long as no two offerings are integrated, and the other offerings are made under Rule 701 or Regulation S (or both). This is common for a rapidly growing company. It is often advantageous to raise capital simultaneously under Regulations D and S. In the former case, the offering will be made only to accredited investors subject to a one-year lock-up period.48 In the latter case, the offerees will be non-U.S. persons who will likewise be subject to a lock-up period of up to one year.49
- Under the Rule 152(b)(4) safe harbor, offers and sales made in reliance on an exemption permitting general solicitation are not integrated if made after any terminated or completed offering.50 Accordingly, a Lab can close one round and then immediately begin another round using Rule 506(c), discussed supra. The

---

[45] *See* Facilitating Capital Formation and Expanding Investment Opportunities by Improving Access to Capital in Private Markets, SEC Release No. 33-10884 (Nov. 2, 2020).
[46] If the first offering is made under Rule 506(c) or another rule that allows general solicitation, then the Lab must have a reasonable belief with respect to each purchaser in the second offering that the Lab or its broker did not solicit the purchaser through general solicitation or established a substantive relationship with the purchaser before the start of that offering. *See* 17 C.F.R. § § 230.152(a)(1), 230.152(b)(1).
[47] *See Id.* § 230.152(b)(2).
[48] *See Id.* § 230.500.
[49] *See Id.* § 230.903.
[50] *Id.* § 230.152(b)(4).

> important point for the practitioner is to make sure that the Lab actually completes or terminates the prior offering—and documents that fact—before starting the Rule 506(c) offering.51

Rule 152 does not by its terms cover commodities, but offers and sales of commodities nonetheless should avoid integration with securities offerings, in the author's view, when they observe these same restrictions. Thus, for example, an offering of tokens that are properly classified as commodities and not as securities should not be integrated with an offering of securities completed more than 30 days earlier, provided that no exemption permitting general solicitation was used in the case of the first such offering to occur.[52] Had Kik's offerings, and Telegram's offerings, not been so close in time to one another, they would not have been integrated, on this view. This point is relevant to Lab capital raising because direct or indirect interests in tokens often are included in those rounds. Professional investors investing in a Lab look to acquire tokens as well as equity.

F. Token Sale and Warrant Terms

There are contracts and arrangements for Labs raising capital that differ from those for other companies. This is because existing or possible future tokens are valuable consideration that can be and are offered to (or solicited by) investors, along with the Lab's more conventional equity and debt securities. Again, a protocol and related tokens at the drawing-board stage, and, for a while thereafter, are presumed to be investment contracts and therefore securities. Term sheets, letters of intent and definitive documents covering tokens to be sold to venture capitalists, angel investors and others as the Lab raises capital touch upon issues covered next.

Form of Token Investment. The Lab might agree to sell tokens that have been created (*i.e.*, tokens that have been emitted, or created, by the protocol), "future tokens" (perhaps using a SAFT), or options or warrants to purchase tokens or future tokens.[53] Lab equity is typically sold to investors in combination with tokens or token warrants.

---

[51] Under Rule 152(d), "the termination or completion of an offering is deemed to have occurred when the issuer and its agents cease efforts to make further offers to sell the issuer's securities under such offering." *Id.* § 230.152(d). It will be obvious that a Lab has done this if and when it sells all of the tokens and other securities to be sold under the offering. Termination short of completion might not be obvious. In either case, it should be documented, and it would be wise to announce that the offering is done.

[52] One should assume that an early-stage Lab offering of tokens is a securities offering. This does not mean that employing Securities Act exemptions for offers and sales of tokens is an implicit admission that the tokens are securities. Anything can be bought and sold under private offering conditions. For example, a case of wine can be offered and sold in compliance with the statutory private offering conditions. There is no need for that, but doing that would not "prove" that bottles of wine are securities, and indeed they are not securities.

[53] For simplicity, options and warrants to purchase tokens are referred to as "warrants" or "token warrants" in the remainder of this chapter.

Years ago, SAFTs were common. The *Telegram* and *Kik* Opinions caused SAFTs to go into decline, as did concern that SAFTs with significant "futurity" might be unlawful futures contracts or swaps.[54] As a result, token warrants are now used more often than SAFTs. Features described below are typical of early-round token sales by Labs, and also, where noted, in token warrants.

Identification of Tokens Being Sold. Unlike stock that is identifiable under a corporation's charter, it is not immediately obvious which tokens are the subject of a Lab's sale to investors. The tokens that are sold or that underlie a token warrant will be defined as digital assets created and issued by the Lab or by an affiliate or founder of the Lab. Certain kinds of tokens are logically excluded from coverage, such as: tokens used solely for development, testing or experimental purposes; tokens issued pursuant to staking, rewards or dilutive controls (so long as the investor is allowed to participate like other token holders and all tokens are diluted equally); and non-fungible tokens issued in arms' length transactions in the ordinary course of business.

Vesting. A warrant may or may not be subject to vesting terms, but tokens underlying the warrant will be fully vested upon issuance to the warrant holder. Likewise, tokens that are purchased outright are normally fully vested. This does not mean they can be resold immediately.

Securities Law Compliance; Resale Restrictions. Again, the tokens discussed in this portion of this chapter are presumed to be securities. Because options and warrants also are securities, an agreement covering the offering, sale and issuance of them will include text evidencing an exempt transaction, such as the absence of Securities Act registration, the need for exemptions, the investor's eligibility to make the investment, and restrictions on resale.[55] Token warrants ordinarily are transferable freely only to affiliates and otherwise subject to the Lab's prior consent (not to be unreasonable withheld). Token resales probably will be limited to specified increments over a multi-year period, typically beginning a year after the date of token issuance. The one-year mandatory lock-up would assure compliance with SEC Rule 903(b)(3)(iii) in the case of

---

[54] Fungible tokens are usually "commodities" under the CEA because they are "interests in which contracts for future delivery are presently or in the future dealt in." 7 U.S.C. § 1a(3). The sale of futures contracts (which excludes "any sale of any cash commodity for deferred shipment or delivery," *Id.* § 1a(12)) are highly regulated under the CEA, as are swaps, and a SAFT could be a "swap" as defined in the CEA (see 7 U.S.C. § 1a(47)(A)). Futures and swaps generally cannot be sold to the public lawfully except on a "designated contract market" such as the Chicago Mercantile Exchange. A SAFT structured with care should not be classified as a futures contract or a swap.

[55] For example, the agreement might include a provision like this: "Purchaser may not transfer any Token unless (1) the Token is registered under the Securities Act and qualified under applicable state securities laws, (2) exemptions from such registration and qualification are available, or (3) the Token is not a security under applicable law." A fungible token that is not a security will nonetheless be a commodity, but sales of commodities in the cash market are little-unregulated.

an off-shore offering[56] and with SEC Rule 144(d)(1)(ii)[57] in the case of all offerings. Token resales might be subject to other conditions imposed, for purposes of legal compliance, by the Lab's board.

Sanctions and AML / KYC Compliance. The investor should expect to represent, warrant and agree that its entry into and performance of the agreement will not cause the Lab to violate U.S. or non-U.S. sanctions laws. The investor also should agree to furnish all information required by the Lab, or by the Lab's agent, relative to AML/ KYC compliance laws, regulations and policies.

Duration. A token warrant typically will expire upon the first to occur of the creation of the tokens and their availability for issuance, the occurrence of an irrevocable decision not to develop any token, or ten years from the agreement date.

Voting Rights and Economic Rights. A well-designed token will not give token warrant purchasers or other token holders any voting rights (such as the right to vote for directors) or economic rights (such as a right to dividends) with respect to the Lab. But the tokens underlying the warrant very likely will have governance rights and economic rights relative to the protocol that emitted them and the ecosystem in which they can be used. Upon exercising a token warrant, the warrant holder would acquire the same rights as any other token purchaser.

Antidilution Protection. The agreement might or might not give the investor a contractual right to acquire additional tokens that later become available, whether or not they have the same features as the tokens first acquired by the investor.

Merger of the Lab with or into another Entity. Because warrants might be sold before the underlying tokens have been created, a token warrant should provide that the investor's rights against the Lab under the agreement should transfer to any successor of the Lab (whether by merger, sale of equity, sale of assets, or consolidation). Anticipating the likelihood that the Lab's business or assets will be transferred to a foundation, the warrant should likewise require the Lab to obtain the foundation's (or a foundation affiliate's) acknowledgment that it is stepping into the shoes of the Lab upon accepting such a transfer.

Deliveries under the Agreement. The purchase price for Tokens is typically paid in U.S. Dollars or in one of several specified stablecoins. The exercise price of a warrant might be payable the same way or instead might be payable in kind. Tokens will be delivered to a wallet address specified by the purchaser.

---

[56] Section 903 imposes a one-year distribution compliance period in the case of an offering of equity securities by a non-reporting company (such as the Lab). 17 C.F.R. § 230.903(b)(3)(iii). One year is the longest such period that is arguably required for an offshore token offering. *See Id.* The SEC has issued no guidance on the applicable distribution compliance period. Some token sellers take the view that their tokens are "debt securities" as defined in Rule 902 because they are not "equity securities" as defined in Rule 405 and that, therefore, they may use the 40-day distribution compliance period under Rule 903 rather than the one-year period.

[57] In the case of a non-reporting company, "a minimum of one year must elapse between the later of the date of the acquisition of the securities from the issuer, or from an affiliate of the issuer, and any resale . . . ." *Id.* § 230.144(d)(1)(ii).

Risks. The investor should expect to expressly acknowledge: the highly speculative nature of the tokens; the financial hazards involved; the lack of liquidity of the tokens and the restrictions on transferability; the qualifications and backgrounds of Lab management; and the tax consequences of purchasing the tokens, without relying upon the Lab or its advisors to understand the same. The investor also should acknowledge that the tokens involve risks, which the investor assumes, including that: (i) the technology associated with the protocol, the tokens and associated ecosystem will not function as intended; (ii) the network will not be completed and the tokens will not be distributed; (iii) the protocol will fail to attract sufficient interest from key stakeholders; (iv) the network will not gain adoption and acceptance; and (v) the Lab, the investor, the network and other persons developing the network may be subject to adverse government actions.

Disclaimers. The Lab should disclaim responsibility for any failure or delay in fulfilling or performing any term of the agreement, including launching, developing and maintaining the protocol and the network, launching the tokens, selling the tokens, sending tokens to the investor's wallet, or distributing the tokens, when caused by *force majeure*. The Lab should also expressly disclaim warranties with respect to the tokens, including any warranty of merchantability, warranty of fitness for a particular purpose, warranty or title, or warranty against infringement of intellectual property rights.

G. Use of Tokens for Incentive Compensation

Ancillary to capital raising, tokens are used as incentive compensation for Lab employees and consultants. In *Ripple Labs*, the district court help that using tokens for compensation is not a securities offering.[58] This specific holding of that court is questionable in light of other decisions[59] and should not be relied upon as a general rule. As in the case of private offerings, though, again there is an applicable Securities Act registration exemption, which in this case is Rule 701.

As applicable here, Rule 701 exempts, from Securities Act registration, offers and sales of tokens that are securities under a written compensatory plan (or written compensation contract) established by a Lab for participation of its employees, directors, officers, consultants and advisors. Critically, the exemption covers consultants and advisors only if they provide *bona fide* services to the Lab and those services are not in connection with capital raising or promotion or maintenance of a market for the Lab's securities (which would include a market for its tokens).[60] There is a formulaic limit on the amount of securities that may be sold under Rule 701, but it is none too

[58] *See* SEC v. Ripple Labs, Inc., *supra* note 4 (S.D.N.Y. July 13, 2023), at 26-27.
[59] *E.g.*, Foltz v. U.S. News & World Report, 627 F. Supp. 1143, 1158 (D.D.C.) (no *Howey* "investment" unless "the compensation package as a whole exhibit[s] 'the characteristics of a security'").
[60] *See Id.* § 230.701(c)(1).

restrictive in practice.[61] A copy of the plan or contract must be delivered to investors. Additional disclosures are required if the aggregate amount of tokens sold in any consecutive twelve month period exceeds $10 million.[62] Rule 701 offers and sales are not integrated with other offerings,[63] but tokens acquired under Rule 701 are "restricted securities" that need to be resold under Rule 144 or under another Securities Act exemption.[64]

Accordingly, the basic requirements are that there must be a plan or agreement covering the tokens and that only employees, directors and officers are eligible, along with consultants and advisors performing *bona fide* services unrelated to capital raising or the capital markets. Questions arise when clients want to stretch the pool of offerees beyond these categories by including affiliates, which is lawful;[65] or by including sellers of goods or mere investors, which are not covered by Rule 701. Sellers of goods and mere investors might be eligible to participate in a concurrent private offering. If not, then no exemption would cover them.

Another question that arises in the Rule 701 context is the tax treatment of the tokens. Section 83 of the Internal Revenue Code will tax as ordinary income the difference between any purchase price paid in cash by the employee or consultant for the tokens and the fair market value of the tokens at the token grant date (which should be structured to be the token launch date).[66] The plan or contract should provide that the Lab need not release tokens to the participant until the participant has made acceptable arrangements to pay any tax required to be withheld. To that end, the participant should agree to authorize withholding from payroll or any other payment due from the Lab to satisfy any withholding obligation, and the participant should authorize the Lab to withhold from delivery to the participant whatever amount of participant's tokens may be required to be withheld by the Lab to satisfy its withholding obligations under the Code or other applicable law.

H. Moving Off-Shore to a Shareholder-Less foundation

Whether or not the Lab was organized in the United States, as its work force of employees and consultants nears completion of the protocol the Lab needs to migrate the business outside the United States because there will be a public token offering structured to comply with Regulation S. Regulation S is more easily satisfied if the token seller is outside the United States.

---

[61] *See Id.* § 230.701(d).
[62] *See Id.* § 230.701(e).
[63] *See Id.* § 230.701(f).
[64] *See Id.* § 230.701(g). The tokens could instead be resold on a Securities Act registration statement, but that theoretical option is impractical under current law and SEC practice.
[65] *See* 17 C.F.R. § 230.701.
[66] 26 U.S.C. § 83.

A U.S.-domiciled Lab is not a foreign issuer, let alone a foreign private issuer, but certain kinds of Regulation S offerings can be made only by foreign issuers and foreign private issuers. It also may be easier to conduct an "offshore transaction" and to avoid "directed selling efforts" if launching from outside the United States.[67]

The reason for offering under Regulation S is that the protocol and token at the time of launch might not be "sufficiently decentralized" or "fully functional" as explained in "When Howey Met Gary (Plastic)." If not, then a securities offering is being made. That securities offering would be exempt from Securities Act registration if made in compliance with the conditions of Regulation S.

The Lab itself need not move and may remain in business perpetually. Even after the public token offering conducted in compliance with Regulation S, the Lab can continue to operate. In other words, its employees can continue to work in the United States, using Lab offices and facilities located there. The best use of Lab personnel beyond this point is probably the invention of new protocols, unrelated to the one that has been moved offshore. Another more sensitive use is the provision of services needed by the foundation or the ecosystem that the foundation has been established to promote, under contract with a subsidiary of the foundation (if not the foundation itself) or with token holders that are or may come to be functioning as a formal or informal decentralized autonomous organization (a "DAO").

The foundation itself will undergo a process and a transformation. Initially it may have only one director, who may be affiliated with the Lab. With a view to decentralization, however, the foundation should wind up with this structure:

- Its governing board should have a majority of members having no affiliation with the Lab or APs and who cannot be removed by the Lab or APs, except perhaps for cause;
- Its charter, or constitution, should require the foundation, its board, its managers and employees to promote the best interests of the protocol and the ecosystem (the token community); and
- To that end, the charter should require or at least permit the board to take instructions from the token community to the full extent permitted by applicable law (which will be the law of the foundation's domicile).

The foundation will likely organize one or more wholly-owned subsidiaries domiciled in crypto-friendly jurisdictions. Examples of such jurisdictions, which vary over time as the law evolves, are the British Virgin Islands (the "BVI") in the Americas and Switzerland in Europe. The choice is best made with reference to the ease of offering tokens under local law at the time of offering and the familiarity (and comfort) of prospective token purchasers with the chosen domicile. For example, American

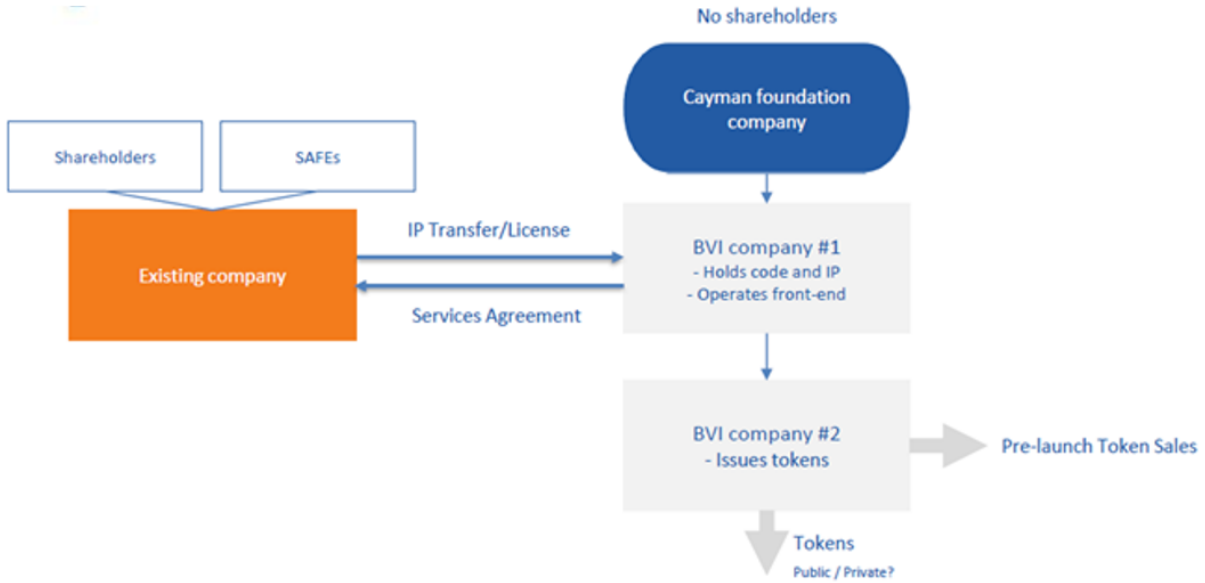
[67] For the applicable requirements of Regulation S, see Section H *infra*.

purchasers tend to be familiar and comfortable with the BVI. European purchasers tend to feel that way about Switzerland.

One foundation subsidiary will later sell tokens to the public in compliance with Regulation S and in furtherance of the tokenomics agreed upon among early investors.[68] Another foundation subsidiary might contract to provide technology services to the token seller or the foundation (or both).

The migration will occur as follows: The Lab will assign the vast majority of its assets, consisting of software code and other IP, to the foundation, retaining only those assets that it needs to remain in operation. After the migration, the foundation will complete the protocol and the preparations for a public token offering in compliance with Regulation S. That offering will be authorized by the foundation board and by the board of the subsidiary that will actually sell the tokens.

This series of transactions, and more, is presented below in an illustration provided by the author's colleague Richard Spencer of the Cayman Islands Bar, as follows:



On the left, there is an existing company, which is the Lab, which in this illustration has issued shares, and also "SAFEs," which are simple agreements for future equity securities. The SAFEs could instead be tokens, or token warrants, but in any event these securities will have been sold in compliance with the securities laws, the Bank Secrecy Act and sanctions laws as explained earlier in this chapter. To avoid any suggestion of integration, the sales of these securities—and of the tokens sold in the Regulation S offering—also will have been timed to conform with the requirements of SEC Rule 152.

---

[68] "Tokenomics" cover matters such as the absolute and relative allocations of tokens among founders, venture investors, management, the general public, the foundation's treasury and the DAO, as well as the increase (by emission) or decrease (by burning) of outstanding tokens and the rate of increase or decrease. Each token and its related protocol essentially will have its own monetary policy, implemented over time with a greater or lesser degree of human involvement.

The foundation in the illustration is organized under Cayman Islands law. A Cayman foundation is a species of company under the Cayman Islands Companies Act (as revised),[69] as well as the Foundation Companies Act 2017 (together, the "Companies Act").[70] Unlike foundations in some other jurisdictions, a Cayman foundation is permitted to carry on commercial activity outside the Cayman Islands. It might instead have been organized under the laws of another jurisdiction that is hospitable to digital assets, such as Switzerland, Dubai, or Hong Kong. Grand Cayman is used in this illustration because it is well-known, it is proximate to the Americas, and it is respected by investors in alternative assets such as investors in hedge funds that are typically offered in two tranches: one being a domestic fund targeting U.S. investors, the other being a Cayman Islands fund targeting non-U.S. investors. The Cayman Islands have an earned reputation for financial sophistication and consistent application of the rule of law—stability—owing in part to their English heritage.

A Cayman foundation may be established with or without equity capital. No minimum amount of capital is required by law.[71] A Cayman foundation is incorporated with one or more members.[72] Once formed, a Cayman foundation can cease to have members at any time.[73]

So the Lab, or a shareholder or other affiliate of the Lab, will initiate the formation of the Cayman foundation, becoming its first and only member. But after that the member could, and ideally should, terminate its membership so as to further the foundation's independence from the Lab and thus further the decentralization of the protocol and token. Cessation of membership will not affect the foundation's existence, capacity or powers, provided that it continues to have one or more "supervisors."[74] A supervisor is a person with no ownership or economic entitlement in the foundation who acts as a steward, ensuring that the directors observe their duties under the foundation's constitution and bylaws.[75] A Cayman foundation that has ceased to have members may not later admit members, or issue shares, unless expressly authorized to do so by its memorandum and articles of association.[76]

The charter, or constitution, of a Caymans foundation consists of its memorandum and articles of association.[77] This constitution can give rights, powers or duties to any person.[78] These might relate to amendment of the constitution or of any bylaws that the

---

[69] Foundation Companies Law, (2017) § 3(2) EXTRAORDINARY GAZETTE (Cayman Is.).
[70] *Id.* § 3(1).
[71] The Foundation Companies Law does not prescribe any minimum capital requirements. *Id.*
[72] *Id.* § 5(1).
[73] *Id.* § 8(1).
[74] *Id.* § 8(2).
[75] *Id.* Schedule 2.
[76] *Id.* § 8(5).
[77] *Id.* § 2(1) ("'[C]onstitution' means the memorandum and articles of a foundation company, but not its bylaws.").
[78] *Id.* § 7(1).

foundation might choose to adopt.[79] Powers given by the constitution may be exercised for any purpose; they need not be exercised in the interest of the foundation itself.[80] Bylaws can, and ideally should, be drafted to cover important aspects of protocol and token governance, including requirements for the board to implement DAO proposals (subject to compliance with the constitution, applicable law and fiduciary duties).

Various persons have roles in and about a Cayman foundation. In addition to the "supervisor," a "secretary" must be appointed by the Cayman foundation, and the secretary must be a "qualified person" licensed or permitted under the Cayman Islands Companies Management Act to provide company management services and to maintain the books and records of the foundation.[81] The registered office of the foundation will be the secretary's business address in the Cayman Islands.

A Cayman foundation will be managed by its board of directors.[82] There are no residency requirements for directors, nor any other restrictions as to who a director may be. That said, it is common for at least one director to be "on island" in order to facilitate timely handling of foundation business that requires on-island attention. The standard of care applicable to the directors of a Cayman foundation is the same standard that would apply to the directors of any other Cayman Islands exempted company, and directors of a Cayman foundation owe the same duties to the foundation that the directors of any other Cayman Islands exempted company would owe to that company.[83]

Only interested persons have information rights and enforcement rights against the foundation under Cayman Islands law. Interested persons are members (of which there should be none after formation), supervisors (or those entitled to be supervisors) and any person so named in the constitution. Beneficiaries are not interested persons. As a result, the foundation and its board are not accountable under Cayman Islands law to many persons.[84] The Cayman Islands has no corporation tax, income tax, capital gains tax, inheritance tax, gift tax, wealth tax or other tax applicable to a company conducting off-shore business. A Cayman foundation is exempt from any Cayman Islands income tax or capital gains tax and can obtain a tax undertaking certificate from the government

---

[79] *Id.* § 7(2).
[80] *Id.* § 7(3).
[81] *Id.* § 4(1)(d).
[82] *Id.* § 7(1).
[83] The duties owed by a director of a Cayman Islands company divide into statutory duties, quasi-contractual duties arising under the company's constitution, fiduciary duties and the duty at common law to exercise reasonable care, skill and diligence. Statutory duties derive from the Companies Act and any other statute to which the relevant company may be subject by virtue of the nature of its business. Duties owed by a director as a fiduciary or as a result of the common law duty of reasonable care, skill and diligence do not derive from (and are not codified in) any statute, but from case law.
[84] Accountability under other laws, such as the U.S. federal securities laws and the Bank Secrecy Act, is possible, though, unless the foundation and its board and affiliates take care lawfully to avoid those laws or else to comply with them.

guaranteeing no change in its tax status for up to thirty years from the date of the undertaking.85

Significantly, a Cayman foundation typically has no shareholders and is instead limited by guarantee (usually a nominal sum).86 Accordingly, it cannot credibly be alleged that it is controlled by a majority shareholder or by a control group of shareholders—there are none. As noted earlier, the foundation will have a board of directors, but it, too, will be outside the control of the Lab and its controlling shareholder(s) when the Regulation S offering occurs. It will be outside their control because a minority of the directors, at most, will be affiliated with them.

The articles and memorandum of association of a Cayman foundation should include the following provisions in order to optimize management of the foundation to fit a protocol development and token offering program:

- Referring in the articles to the protocol and ecosystem under development, the "objects" of the foundation should specifically include development, and incentivizing growth, of the protocol's DAO, its decentralized network and that ecosystem.
- Under the memorandum of association: a specified founder or the founder's successor may have the power or right to appoint or remove directors and to adopt, revoke or modify bylaws; subscribers should be given the right to appoint the first directors; the founder or successor, should there be none, then a named supervisor, should have the power to appoint or remove directors; should there ever be no founder, successor or supervisor in place, the directors themselves should have the power to appoint directors.[87]
- Under the memorandum of association, the directors should be directed to report to the founder, successor or supervisor concerning the business and affairs of the foundation, the discharge of their duties and the exercise of their powers.
- Under the memorandum of association: the first supervisor would be appointed by the subscriber(s), but the founder (should there be one) also should have the right to appoint or remove the supervisor(s); and the foundation should be required at all times to have at least one supervisor, who should have the right to require access during normal working hours to the books and records of the foundation.
- The foundation may, but need not, have beneficiaries. Naming beneficiaries is disfavored.
- The foundation should be required to have an annual meeting, attended by the founder (should there be one), any members (of which there should be none),

[85] Tax Concessions Law, (2018) § 4 EXTRAORDINARY GAZETTE (Cayman Is.).
[86] Foundation Companies Law, (2017) § 4(1)(a) EXTRAORDINARY GAZETTE (Cayman Is.).
[87] *Id.* § 7.

any beneficiaries to whom that right may be granted (of which there should be none), the supervisor and the directors.

- The memorandum of association also should include provisions covering: amendment of the articles and memorandum of association; the liquidation and winding up of the foundation (including the charities or other persons to which payment of any surplus assets should be made); the election of officers by the directors; the adoption of bylaws by the directors; and the indemnification by the foundation of every founder, successor, supervisor, director, secretary and other officer of the foundation and the exoneration of all such persons from liability.

The illustration above also refers to two companies domiciled in the BVI, which are a direct and an indirect wholly-owned subsidiary of the foundation. These subsidiaries are depicted as domiciled in the BVI because its Virtual Asset Service Providers Act, 2022 (the "BVI VASP Act"), in contrast to Cayman Islands law, does not, in respect of the definition of a virtual assets service, capture the issuance of tokens on the issuer's own behalf, or the private or public sale of tokens (or any other proprietary trading activities involving digital assets). In addition, the BVI VASP Act provides that a person who engages in or performs any of the following activities shall not qualify to be treated as a virtual assets service provider: (a) solely creating or selling a software application or virtual asset platform; or (b) solely engaging in the operation of a virtual asset network without engaging or facilitating any of the activities or operations of a VASP on behalf of customers.[88]

Following recommendations made by the Financial Action Task Force, the Cayman Islands adopted the Virtual Asset (Service Providers) Act in 2020 (the "Cayman VASP Act").[89] The Cayman VASP Act provides for the regulation of virtual asset businesses and for the registration and licensing of persons providing "virtual asset services,"[90] and, accordingly, is less flexible than BVI law for the purposes of token sales. The BVI subsidiaries, being foundation assets, will nonetheless be managed by foundation personnel.

---

[88] Virtual Assets Service Providers Act, (2022) § 2(1) OFF. GAZETTE (Virgin Is.) ("'VASP', subject to subsections (2), means a virtual asset service provider who provides, as a business, a virtual assets service and is registered under [the Virtual Assets Service Providers Act] to conduct one or more of the following activities or operations for or on behalf of another person[:] (a) exchange between virtual assets and fiat currencies; (b) exchange between one or more forms of virtual assets; (c) transfer of virtual assets, where the transfer relates to conducting a transaction on behalf of another person that moves a virtual asset from one virtual asset address or account to another; (d) safekeeping or administration of virtual assets or instruments enabling control over virtual assets; (e) participation in, and provision of, financial services related to an issuer's offer or sale of a virtual asset; or (f) perform such other activity or operation as may be specified in [the Virtual Assets Service Providers Act] or as may be prescribed by regulations made under section 47.").

[89] *See* Virtual Asset (Service Providers) Act, (2020) LEGIS. GAZETTE (Cayman Is.); Virtual Asset (Service Providers) (Amendment) Act, (2020), LEGIS. GAZETTE (Cayman Is.).

[90] *See* Virtual Asset (Service Providers) Act, (2020) Preamble LEGIS. GAZETTE (Cayman Is.)

One BVI subsidiary directly owned by the foundation (BVI company #1 in the illustration) will enter into a contract or contracts with the Lab pursuant to which the Lab will transfer its intellectual property to BVI subsidiary #1 and will agree to provide some measure of technology support and other services for BVI subsidiary #1, ending upon the launch of the Regulation S offering or, in any event, upon the expiration of the applicable Regulation S distribution compliance period.[91] BVI subsidiary #1 will hold the software code for the protocol and the token and will operate the front end of the technology stack.

The other BVI subsidiary (BVI company #2), a direct subsidiary of BVI company #1, will become the token seller in the Regulation S offering. It may also sell tokens privately before that offering, taking care (as all these entities must) to avoid integration. Some token offering programs combine the functions of BVI company #1 and BVI company #2 into a single BVI subsidiary of the foundation, but it is better to use two subsidiaries rather than one in order to ring fence the IP rights (held by BVI company #1) from the litigation and regulatory risks inherent in the sale of tokens (undertaken by BVI company #2).

By making a token offering under Regulation S, BVI company #2 will be furthering the decentralization of the protocol and token. This assumes that there will be many buyers who are unaffiliated with the Lab and other APs, which should be the intention. Buyers who are customers of a well-managed, regulatory-compliant, prominent exchange will have been curated by the exchange for their domiciles (which need to be not only non-U.S., but also must be outside other countries that restrict crypto offerings severely, such as Canada and the PRC). The resulting pool of offerees will be buyers residing on multiple continents that not only are unaffiliated with the Lab and other APs but also are unaffiliated with one another.

A DAO needs to come into existence and needs to govern the operation of the protocol and token, including, significantly, the repair of any software bugs and the improvement of the protocol and the development of the ecosystem, as and after the token is sold under Regulation S. As there must be a first mover, the Lab will take the leadership in this regard, but it cannot remain the driving force in the DAO or otherwise drive the governance of the protocol and the token if they are ever to become sufficiently decentralized. Similarly, the protocol and token might need further development after the Regulation S offering in order to become fully functional.

A protocol and token that is either sufficiently decentralized or is fully functional is not an investment contract, in the author's view. But it takes time to develop either or both of those characteristics. The beauty of the Regulation S offering is the mandatory post-offering period during which resales to U.S. persons are impeded, or even blocked.

---

[91] The reason for terminating support at that time is to further the decentralization and the full functionality of the protocol and the token. If services by the Lab are critical to the operation of the protocol after the Regulation S offering ends, then it is likely that the protocol and the token are not fully functional at that time and are not sufficiently decentralized then in a "When Howey Met Gary (Plastic)" sense.

Such resales will be blocked if the buyers can transfer only to persons who have been verified as non-U.S. persons. And transfer to non-U.S. persons for a period of a full year will, at the end, result in a greater degree of decentralization, and a higher degree of functionality, than where the protocol, token and ecosystem began. Off-shore lock-up for longer than a year will result in still greater decentralization and functionality.

The expiration of the Regulation S distribution compliance period heralds permission for free resale to U.S. persons because of compliance with the requirements of the exemption. But it may also and more importantly allow the foundation board to conclude that the protocol, token and ecosystem have become sufficiently decentralized or fully functional (or both). In that case, unless there is some other reason to conclude that the arrangement is a "security," as in the case of a "note" that is a security, then the foundation board could rightly determine that the protocol and token have mutated into a non-security commodity, like Ether did, and could authorize BVI company #2 to sell additional tokens without bothering to comply with Regulation S or any other Securities Act exemption.

Two examples of sellers reaching this conclusion under similar circumstances are Stacks and Polkadot. Stacks were initially offered and sold in compliance with Regulation A.[92] The token issuer continued to develop the ecosystem, and the token became decentralized. At a certain point, the issuer enlisted its outside counsel to analyze the status of the protocol and token under the securities laws. Based on a detailed, thoughtful analysis of its legal counsel, the issuer's board determined that its protocol and token were not securities and curtailed further securities law compliance efforts.[93]

Polkadot was another such case. Polkadot tokens were first publicly offered solely to non-U.S. persons in a Regulation S offering in which the tokens were delivered pursuant to claims made only by the original subscribers.[94] The initial distribution of tokens occurred in October 2017. Through public and private Dutch auction sales, the foundation raised $145 million in Ethereum.[95] The initial total Token supply was set at 10 million tokens, but, following a community vote, the cap was removed.[96] After additional private sales in 2019 and 2020, Tokens were allocated to five groups:[97] (i) 50%

---

[92] Blockstack PBC Regulation A Offering Statement (Form 1-A) (July 8, 2019).

[93] Robert Rosenblum, Amy Caiazza & Johanna Collins-Wood, *Summary of Memorandum Regarding the Stacks Tokens* (Dec. 2, 2020), https://blog.blockstack.org/stacks-cryptocurrency-expected-to-reach-non-security-status-in-the-united-states.

[94] *See Introduction to Polkadot (DOT)*, BITGET, https://www.bitget.com/academy/Introduction-to-Polkadot (last visited, July 27, 2023) ("Participants were required to use a KYC system called PICOPS, which verifies the identity of each participant. Participants that were unable to verify themselves were deemed ineligible. The sale was also not available to any Chinese or American citizens due to regulatory concerns.").

[95] *See Id.* The private sale raised $80 million and the public sale raised $65 million.

[96] See *Id.*

[97] *See Id.*; *see also Polkadot*, COINGECKO, https://www.coingecko.com/en/coins/polkadot/tokenomics (last visited July 27, 2023).

to the initial investors; (ii) 5% to the 2019 private sale investors; (iii) 3.4% to the 2020 private sale investors; (iv) 11.6% to the foundation for future fundraising efforts; and (v) 30% to the foundation to further develop the Protocol and for "other undisclosed foundation activities."[98] The 11.6% allocation retained by the foundation probably diminished over time, based on additional private fundraising efforts undertaken since the 2020 private sale.[99] The active participants, or APs, led by Gavin Wood, who had also co-founded Ethereum, retained a portion of the tokens allocated to the foundation, but Mr. Wood no longer is associated with the foundation so his token holdings are unknown. The APs always held or controlled less than 20% of the tokens outstanding. The protocol's and tokens' main features, and any changes to them, are managed by the protocol's governance system, which is highly decentralized. Mr. Wood remains the majority shareholder of the lab and has said that he will "retain the title of Chief Architect"[100] of the token and protocol and will remain focused on making the token and protocol "more relevant to large swathes of the population."[101] Notwithstanding his continuing role as a master coder, the token and protocol are fully developed and are functioning as intended. The Polkadot protocol is a leading L1 public blockchain. It seems clear that the token's and protocol's standing within the industry would not change if Mr. Wood were gone. In other words, Polkadot passes the Bahamas test.[102]

Based on these facts, among others, the foundation concluded that Polkadot had morphed from an investment contract into a non-security commodity. It consulted with

---

[98] *See* supra note 94.

[99] *See* Polkadot *Funding Rounds*, CRUNCHBASE, https://www.crunchbase.com/organization/polkadot/investor_financials (last visited July 27, 2023) (showing an additional seed round undertaken in 2021, but limited information on specific token allocations for this private sale).

[100] *See* @gavofyork, TWITTER (Oct. 21, 2022, 10:51 AM), https://twitter.com/gavofyork/status/1583516332515282944?lang=en.

[101] *See* Danny Nelson, *Polkadot Co-Fonder Gavin Wood Steps Down from CEO Role at Blockchain's Builder*, COINDESK (Oct. 21, 2022, 8:44 AM), https://www.coindesk.com/business/2022/10/21/polkadot-co-founder-gavin-wood-steps-down-from-ceo-role-at-blockchains-builder-report/ (last visited July 27, 2023).

[102] See M. Todd Henderson & Max Raskin, A Regulatory Classification of Digital Assets: Toward an Operational Howey Test for Cryptocurrencies, ICOs, and other Digital Assets, 2019 COLUM. BUS. L. REV. 444, 461 (2018) ("The Bahamas Test asks: 'If there is a minting and selling of an instrument, as opposed to open mining of it, is there either an explicit or implicit contract to build and manage software such that if there were a breach of that contract, the project would fail? If there is no such sale or if there is no such obligation, then the "efforts of others" prong of the test is not satisfied and the instrument is not a security.' Said differently: if the sellers fled to the Bahamas or ceased to show up to work—like Satoshi Nakamoto—would the project still be capable of existing? If the answer is 'yes,' then the risk of fraud is sufficiently reduced such that the instrument is not a security."); see also SEC v. Telegram Grp. Inc., 448 F. Supp. 3d 352 (S.D.N.Y. Mar. 24, 2020) ("The Court finds that if, immediately after launch, Telegram and its team decamped to the British Virgin Islands, where Telegram is incorporated, and ceased all further efforts to support the TON Blockchain, the TON Blockchain and Grams would exist in some form but would likely lack the mass adoption, vibrancy, and utility that would enable the Initial Purchasers to earn their expected huge profits. Initial Purchasers' dependence on Telegram to develop, launch, and support the TON Blockchain is sufficient to find that the Initial Purchasers' expectation of profits was reliant on the essential efforts of Telegram." (citing Henderson & Raskin, supra)).

the SEC Staff at length about that conclusion and its reasoning. No no-action letter was issued by the SEC Staff, but neither did the SEC contradict the foundation's published claim that the token had morphed and is no longer a security.[103] The foundation kept the SEC Staff apprised of its process every step of the way. Given the token's prominence in the industry, one would expect the SEC to issue a statement disagreeing with the foundation's claim if it did disagree. In these particular circumstances, the SEC's inaction is fairly construed as implicit agreement with the foundation's "non-security" conclusion.

As in the cases of Stacks and Polkadot, it should be the foundation board that considers over time whether the protocol and the token have mutated from an investment contract into a non-security commodity. The board should make such a determination, if at all, only in close consultation with legal counsel who are expert in digital asset securities law matters, in reliance upon such counsel's opinion.

I. Regulation S Token Offerings

The SEC adopted Regulation S in 1990 to provide safe harbors from Securities Act registration requirements for offshore offers and sales of securities.[104] In doing so, the SEC enhanced access to offshore markets for both foreign and domestic issuers.[105] The basic approach of Regulation S is territorial. It limits the protective reach of registration to investors that are offered and sold securities within the U.S. market, rather than protect U.S. offerees and purchasers worldwide. In the SEC's view, "principles of comity and the reasonable expectations of participants in the global markets" dictated its decision that "laws applicable in jurisdictions outside the United States [would] define requirements for transactions effected offshore."[106]

In other words, the thrust of Regulation S is that investors choose the laws that apply to their investment decisions by picking the market in which they choose to invest. For example, U.S. citizens living and working in Paris who buy securities on Euronext Paris are not protected by the Securities Act, but rather must look for their protection to EU law, even as their French neighbors do. French citizens who live and

---

[103] *See* Daniel Schoenberger, *Less Trust, More Truth: Polkadot's Native Token (DOT) Has Morphed and Is Not A Security. It Is Software.*, MEDIUM (Nov. 4, 2022), https://medium.com/web3foundation/less-trust-more-truth-polkadots-native-token-dot-has-morphed-and-is-not-a-security-b2a8847a70cc (last visited July 27, 2023) ("[W]e are pleased to announce that [the Token], the native digital asset of the [Protocol], has morphed. In our view, current day offers and sales of [the Token] are not securities transactions, and [theToken] is not a security. It is merely software."). The SEC has neither confirmed nor denied that view, publicly. In his article, Mr. Schoenberger details that the foundation has been in communication with the SEC's FinHub staff for more than three years regarding the Token and its security classification thereof. *Id.*

[104] *See* Offshore Offers and Sales, SEC Release No. 33-6863, 2 (Apr. 24, 1990).

[105] *See* Offshore Offers and Sales, SEC Release No. 33-7505 (Feb. 17, 1998).

[106] Offshore Offers and Sales, *supra* note 104, at 5.

work in the United States are protected by the Securities Act, just as U.S. citizens and residents are.

Regulation S is not one exemption, but rather several different exemptions, each of which is applicable (or not) in different circumstances. These exemptions are useful in token offerings when the tokens are, or might be considered, securities. Except for a handful of tokens, that is always a possibility, particularly when the protocol and token are in their early days of adoption and use.

The various registration exemptions and how they can be used for token offerings will be described. All of this analysis is presented without written SEC Staff guidance in the digital asset era, as there has been no such guidance despite requests for written guidance.

As stated in Rule 901 of Regulation S, "the terms offer [and] sell . . . shall be deemed to include offers and sales that occur within the United States and shall be deemed to exclude offers and sales that occur outside the United States."[107] This "general statement" that frames the regulation potentially exempts a broad variety of offerings, but it is strict. Some counsel rely upon it to exempt offerings that do not target U.S. markets or U.S. persons, particularly if launched from off-shore and if attempts are made to prevent U.S. persons from subscribing. Other counsel steer their clients to one or more of the other Regulation S exemptions because of the possibility that one sale, or even one offer, within the United States would damage a Rule 901 exemption claim. Their concern is that attempts to avoid U.S. markets and U.S. persons might not be fully successful, in which case the exemption might be deemed unavailable. The burden is on the person claiming the exemption to prove that the conditions of the exemption were satisfied, so the token seller would need to be able to show that no offers occurred in the United States, which might be hard to prove. The use of social media would raise an issue under Rule 901 because of the likelihood that U.S. markets would be touched and U.S. persons would be offered the token.

The three more-detailed exemptions beyond the Rule 901 "general statement" are found in categories of Rule 903. There are two universal conditions that must be satisfied in each of the three categories. First, the offering must be an "offshore transaction"; *i.e.*, the offer must not be made to a person in the United States and either the buyer must be outside the United States or else the seller or its agent must reasonably believe that the buyer is outside the United States. This condition can be satisfied in the case of a token offering by taking care to perform KYC checks on all persons before they become offerees and by excluding all persons whose information discloses a United States location.

In Commodities Futures Trading Comm'n v. Zhao and SEC v. Binance, the government alleged that Binance actively circumvented bans on trading in the United States by encouraging United States customers to falsify their locations in the KYC

[107] *See* 17 C.F.R. § 230.901.

process.[108] Needless to say, if such is the case, that won't work. Rather, the seller or its agent must take care to exclude persons in the United States from the transaction. Persons who are identified upon establishment of a relationship as being in the United States must be excluded.

The second universal condition is that there must be no "directed selling efforts" by the issuer, any distributor, any affiliate, or any agent for any of them; in other words, no activity can be "undertaken for the purpose of, or that could reasonably be expected to have the effect of, conditioning the market in the United States for any of the securities being offered in reliance on" Regulation S.[109] The regulatory definition of "directed selling efforts" is elaborated in terms of what publications, what advertisements, what press conferences, research reports and the like are, and are not, permitted.[110] This is not helpful in the digital age, let alone the blockchain technology age. Probably the definition of "directed selling efforts" should be updated, as when it was adopted there was no such thing as blockchain technology. As it is, token sellers advised by competent counsel will avoid directed selling efforts by blocking communications to computers identifiable to United States addresses or by contracting with exchanges and other purchasers to do the same. Some go so far as to avoid token program disclosures in the English language.

Again, these universal conditions—the "offshore transaction" mandate and the "directed selling efforts" ban—apply to all three categories of offerings under Rule 903. The universal conditions can be satisfied by conscientious sellers and their counsel as explained above.

Category 1 of Regulation S, found in Rule 903(b)(1), offers two possible exemptions so long as the universal conditions are satisfied and the offering is made by a "foreign issuer." An issuer that is a corporation or other organization incorporated or organized under the laws of a foreign country is a "foreign issuer."[111] A Cayman Islands foundation would be a foreign issuer, as would a BVI subsidiary of such a foundation.

Such an offering will be exempt if there is no "substantial U.S. market interest" in the tokens (*i.e.*, no "SUSMI") at the commencement of the offering. This "no SUSMI"

---

[108] Complaint, Commodity Futures Trading Comm'n v. Zhao, No. 1:23-cv-01887 (N.D. Ill. Mar. 27, 2023); Complaint, SEC v. Binance, No. 1:23-cv-01599 (D. D.C. June 5, 2023).

[109] 17 C.F.R. § 230.902(c)(1).

[110] For example, placing an advertisement in a publication with a general circulation in the United States that refers to the offering being made under Regulation S is considered directed selling efforts. But a tombstone advertisement subject to strict content limitations might be acceptable. *See Id.* § 230.902(c)(1)–(3). The author's view is that, ideally, a Rule 903 offering should not be noticed in the United States at all. In other words, a person searching the internet from the United States might be able to determine that a Rule 903 offering is underway but should not be able to determine its details (or to participate in it).

[111] *See Id.* § 230.903(b)(1) (the "no SUSMI" exemption); *Id.* § 230.903(b)(2) (the "overseas directed offering" exemption); *see also Id.* § 230.405 (defining "foreign issuer" as "any issuer which is a foreign government, a national of any foreign country or a corporation or other organization incorporated or organized under the laws of any foreign country").

condition is easily satisfied in the case of a crypto asset offering. SUSMI is defined in terms of United States securities exchange and inter-dealer quotation system volumes in the case of tokens that are equity securities[112] and in terms of the number of record holders and the outstanding principal amount of holdings by U.S. persons in the case of tokens that are debt securities. These conditions can be monitored such that the limits are never breached.

The other Category 1 exemption is for an "overseas directed offering" by the foreign issuer. This kind of offering by the Cayman Islands foundation or BVI subsidiary will be exempt if it is "directed into a single country other than the United States to the residents thereof and that is made in accordance with the local laws and customary practices and documentation of such country. . . ." The "single country" condition might seem to be challenging because crypto asset purchasers, like the internet, are global. The SEC Staff have construed the "single country" requirement to include the entire European Union as a single country.[113]

So a crypto offering to EU residents only would seem to be an overseas directed offering, if conducted in accordance with local law, customary practice and documentation. The adoption of "MiCAR" by the EU is encouraging in this regard, as it promises to enable crypto offerings there.[114]

A simpler way to satisfy the "one country" requirement is to direct the offering into a single country that liberally permits token sales, locking up the tokens in a wallet controlled only by residents of that country, and requiring by contract that a full year pass before resales to non-residents are allowed.

Category 2 is more complex. For one thing, it can be used only for "debt securities" of a "foreign private issuer." The classification of tokens as "debt securities" versus "equity securities" is discussed elsewhere.[115] Of course the universal conditions also apply. And there are two additional conditions, as follows.

First, "offering restrictions" must be implemented. This means that all offering materials and documents (other than press releases) used before the expiration of a 40-day "distribution compliance period" must state that the tokens have not been registered under the Securities Act and may not be offered or sold in the United States or to U.S. persons unless registered under the Securities Act or a registration exemption is available. These statements must be made prominently in any offering materials and

---

[112] *See Id.* § 230.902(j).

[113] See Securities Act Compliance and Disclosure Interpretation 277.02 (last updated Nov. 20, 2023), https://www.sec.gov/corpfin/securities-act-rules.htm#277.02.

[114] "MiCAR" is an acronym for "markets in crypto-assets regulation," an EU-level framework for the regulation of such assets. *See* Council of the European Union, Digital Finance: Council Adopts New rules on Markets in Crypto-Assets (MiCA) (May 16, 2023).

[115] *See* note 56 supra and text accompanying notes 127-28 *infra*.

in any advertisement. They can be coded into the token itself (although the coders will resist that approach because it's inefficient).[116]

Second, any offer made before the 40-day period expires must not be made to a U.S. person or for the account or benefit of a U.S. person.[117] In general, a "U.S. person" is any natural person resident in the any of the United States, its territories or possessions or the District of Columbia, any partnership or corporation organized under the laws of the United States, and certain other persons.[118] This requirement can be satisfied by locking up the tokens for 40 days. Some exchanges allow trading on the exchange among non-U.S. persons during the lock-up period. They can determine the residences of their customers through KYC procedures.

There also is a special rule for "distributors," which are underwriters, dealers and selling agents participating in the distribution.[119] The rule is that a distributor selling to a distributor, dealer or person receiving remuneration during the distribution compliance period shall send a confirmation or other notice to the purchaser stating that the purchaser is subject to the same restrictions on offers and sales that apply to a distributor. The crypto industry does not use trade confirmations because trades settle immediately on a "T+0" basis, but notices can be delivered as part of a token's code.

For avoidance of avoidable burdens, it is best to minimize the use of distributors in a Regulation S token offering. But an exchange or market maker might well be a distributor, in which case it would need to comply with the rules applicable to distributors.

The Category 3 exemption applies to tokens that are "equity securities." Again, classification is discussed elsewhere in this chapter. This category imposes the strictest conditions. The universal conditions apply. So do the distribution compliance conditions that apply in Category 2, except that the period for Category 3 is one year rather than 40 days. It is no more challenging to lock up a token for a year than it is for 40 days, but in a hot market one year might seem like forever. And again, there are special rules for distributors in Category 3, which are no different from those in Category 2.

Category 3 adds four more burdens that apply during the one-year distribution compliance period, as follows:[120]

(1) The purchaser certifies that it is not a U.S. person and is not acquiring the tokens for the account or benefit of any U.S. person or is a U.S. person who purchased tokens in a transaction that did not require registration under the Securities Act;

---

[116] *See* 17 C.F.R. § 230.902(g) (defining "offering restrictions"). In the case of an equity offering by a domestic issuer, hedging before the expiration of the distribution compliance period is generally forbidden and the offering materials and documents must say so. Again, this can be coded into the token.
[117] *See Id.* § 230.903(b)(2)(ii).
[118] *See Id.* § 230.902(k).
[119] *See Id.* § 230.902(d).
[120] *See Id.* § 230.903(b)(3).

(2) The purchaser agrees to resell the tokens only in accordance with Regulation S, pursuant to registration under the Securities Act, or pursuant to an available exemption from registration, and agrees not to engage in hedging transactions unless in compliance with the Securities Act;

(3) The tokens contain a legend (if the issuer is a domestic issuer) to the effect that transfer is prohibited except in accordance with Regulation S, pursuant to Securities Act registration, or pursuant to an available registration exemption, and that hedging transactions involving the tokens may not be conducted unless in compliance with the Securities Act.

(4) The issuer, either by contract or in its organizational documents, must refuse to register any transfer of the tokens not made in accordance with Regulation S or pursuant to registration under the Securities Act or pursuant to an available registration exemption; but if the tokens are in bearer form, as will be the case (crypto assets are bearer instruments), then other reasonable procedures (such as a legend described below) shall be implemented to prevent any transfer not made in accordance with Regulation S. The legend would say that transfer is prohibited except in accordance with Regulation S, pursuant to registration under the Securities Act, or pursuant to an available registration exemption; and that hedging transactions may not be conducted unless in compliance with the Securities Act.

Experience suggests that these certifications and agreements can be satisfied with representations and warranties, agreements and other statements included in a token's code (in the case of a token that will be emitted and sold without any paperwork) or in transaction documents that might be used where, for example, the tokens are being sold to only a few purchasers and will be locked up in one or a few wallets for a year. It's awkward, but it's feasible. The "legends" mentioned in the rule are not "placed" on tokens the way they are sometimes still "placed" on stock certificates and bonds, but prominent disclosure of the facts required to be legended by coding them into the token or otherwise disclosing them to offerees should suffice.

The special rules for "distributors" in Categories 2 and 3 are as follows: First, the universal conditions apply. Second, each distributor must agree in writing that all offers and sales during the 40-day or one-year period, as applicable, shall be made only in accordance with Rule 903 or 904, pursuant to Securities Act registration or pursuant to a registration exemption. And third, each distributor selling tokens to a distributor, dealer or person receiving selling remuneration, during the 40-day or one-year period, must notify the purchaser that it is subject to the same restrictions that apply to a distributor. These "agreements" and "notices" have a "role hole, square peg" feel about them, as they were prescribed in 1989, pre-dating modern information technology, but they can be satisfied using the same disclosure methods described above.

Under SEC Rule 904, a resale by a person other than the issuer, a distributor, an affiliate of any of them, or an agent of any of them, is deemed to occur outside the United States under Rule 901 (and thus is exempt) if made in an "offshore transaction"; if no "directed selling efforts" are made in the United States by the seller, an affiliate or

any agent of them; and if certain additional requirements are satisfied in the case of a resale by a dealer or a person receiving selling remuneration or by an officer or director of the issuer or a distributor.[121] Rather than rely upon Rule 904 to exempt resales, it is better to await the completion of the 40-day or one-year distribution compliance period and then resell.

J. Regulation S Interpretive Issues and Risks

Using Regulation S for a digital assets offering invariably has something of a "round hole, square peg" feel because Regulation S was created at a time when offerings of every variety were literally papered. Not only was there no such thing as blockchain technology, but there were no internet-based offerings to speak of. For this reason, the term "directed selling efforts" is defined in part in Rule 902(c) by forbidding placement of advertisements in newspapers and other publications "with a general circulation in the United States" and the use of carefully worded "tombstone advertisements." "Offering restrictions" are defined in Rule 902(g)(2) with reference to statements appearing in specified parts of the "prospectus or offering circular" used as "offering materials and documents" in connection with the offering.

These provisions of Regulation S seem quaint today, when virtually all securities, even SEC-registered securities, are issued, evidenced and sold using electronic media.[122] They raise significant interpretive issues in connection with digital asset offerings. To date, neither the SEC nor its staff has addressed the use of Regulation S for these offerings, so the interpretative questions identified below have not been addressed by the agency. This section will address the major issues and the primary risks, which are "controlling person" liability and other similar liability risks.

"Flowback" into the United States is the first issue to be addressed. The challenge here is not an interpretive one, as Regulation S does not preclude the resale of securities into the United States. On the contrary, the safe harbors contemplate that it will occur, the main question being when. The challenge is that speedy resale into the United States "in size" might tempt the SEC or the plaintiffs' bar to believe that inadequate (or no) attempts were made to cause the offering to come to rest offshore.

As noted earlier, there is a 40-day distribution compliance period for certain kinds of offerings and a one-year distribution compliance period for others. Clients are advised to contract with initial token purchasers that they will comply with the applicable period. Without more, it is possible that purchasers will breach that promise and resell immediately into the United States. In the author's view, neither the Lab nor the foundation nor any of its subsidiaries is responsible for that result, except perhaps in an

---

[121] *See Id.* § 230.904.

[122] Virtually all SEC-registered securities are held in electronic form at The Depository Trust Company. *See Investor Bulletin*, SEC (July 12, 2023), https://www.sec.gov/about/reports-publications/investor-publications/holding-your-securities-get-the-facts (last visited July 27, 2023).

unusual case where it had reason to believe that the purchasers could not be trusted to honor their promises.

There are steps that can be taken, however, to mitigate or prevent the risk of early flowback. One is to create an economic incentive for the token holders to avoid reselling into the United States prematurely. This can be accomplished by offering a right of redemption at the original offering price during the distribution compliance period, but only for non-U.S. token holders. In doing so, the token seller creates a floor price for the token during the distribution compliance period, but only for non-U.S. buyers. The non-U.S. market price for the token should therefore be higher than any U.S. market price and the tokens should tend to stay outside the U.S., at least for the duration of the redemption right.

Another more direct way to address the possibility of premature flowback is to deliver the tokens, upon closing the Regulation S offering, into wallets that are controlled by a centralized exchange, where the exchange has adopted policies and procedures to prevent transfer, during a specified period, to wallets identified to U.S. persons. Several exchanges have adopted such policies and procedures. They identify U.S. persons in the course of conducting AML / KYC procedures. They can block transfer to such persons and can disable transfer away from the exchange during a specified period. The result is that a Regulation S purchaser that is a customer of such an exchange must be a non-U.S. person and can transfer only to other non-U.S. persons during the relevant period.

An even more direct answer to the flowback issue is to deliver the tokens, upon closing the offering, into a wallet or wallets controlled by non-U.S. persons and to forbid, by contract, any transfer at all for the duration of the distribution compliance period, if not longer. A one-year period for this lock-up is especially good, and this is a true lock-up as not even another non-U.S. person can buy the tokens while they are locked up. The advantage of this approach is that it guarantees that there will be no resales into the United States for the duration of the lock-up. The disadvantage to the initial purchaser is illiquidity, which presumably will be discounted in the purchase price.

There also is a disadvantage for the protocol and the token in that token ownership will not become more decentralized by reason of broad ownership so long as the tokens are locked up. Nevertheless, other progress toward regulatory objectives can be achieved during the lock-up. The functionality of the protocol and the ecosystem can be increased to the point where they are "fully functional" when the lock-up expires even if they were not fully functional upon the closing of the Regulation S offering. In the author's view, a protocol and related token that are fully functional in the way that the Ethereum blockchain and Ether are fully functional are not an investment contract even if they are centralized. Also, and with reference to decentralization, a DAO can be created and can become operational during the lock-up period, and other steps toward

decentralization can be taken.[123] So the contracted lock-up upon closing is an excellent approach, especially for products and services that are close to full functionality or are on the path to DAO formation and management.

This is probably a good place to mention that contacts with U.S.-based exchanges and market makers generally should be avoided. Contacts with non-U.S. exchanges and market makers in the author's view are permissible, and the SEC seems to agree, as in the *Wahi* case it attacked contacts with U.S.-based exchanges only.[124] As for decentralized exchanges, no action is needed (or advisable) by the sell-side of the offering, and no human contact with the exchange is even feasible. Market makers and investors may choose to become liquidity providers in liquidity pools that they can create. The Lab, the foundation, its subsidiaries, and their associated personnel, are all best advised to let that happen (if and when it does) without playing a role in exchange listing or trading themselves.

The SEC plainly views contacts with U.S.-based exchanges as indicative of an investment contract.[125] While "no contact" is preferable, it is probably unrealistic. Any contacts should be initiated by "reverse inquiry" from the exchange. Listings should be proposed by the exchanges, not by the Lab, the foundation, or their personnel. Contracts with detailed terms and conditions should be proposed by the exchanges. Legal counsel to the sell-side will want to make sure that AML / KYC and sanctions compliance is embedded in these contracts, along with Regulation S compliance, CEA compliance[126] and antifraud protections.

Related to contacts with exchanges, there is the question whether an exchange and certain other transaction participants would be considered "distributors." Simply put, while guidance from the SEC is lacking and would certainly be useful, it is possible that exchanges and market makers are distributors for the purposes of Regulation S. When they are, then, to assure the availability of the Regulation S safe harbor, exchanges and market makers need to comply with the Regulation S requirements for distributors when applicable. Rule 902(d) defines "distributor" as "any underwriter, dealer, or other person who participates, pursuant to a contractual arrangement, in the distribution of securities offered or sold in reliance on . . . Regulation S."

In conventional debt and equity securities markets, exchanges are not distributors because they do not participate in the distribution of securities. Investment banks, placement agents and broker-dealers are the distributors. Crypto asset markets are different from conventional securities markets because of the multiple roles played by exchanges. Specifically, they are not only exchanges, but also may perform roles similar

---

[123] Decentralization has many components, only one of which is dispersed token ownership.

[124] *See* Complaint, SEC v. Wahi, No. 2:22-cv-01009-TL (W.D. Wash. July 21, 2022).

[125] *See, e.g.*, *Id.*; SEC v. Ripple Labs, Inc., No. 1:20-cv-10832-AT-SN (S.D.N.Y. Dec. 22, 2020).

[126] The CEA compliance point is to block the exchange by contract from creating derivatives or swaps. This is important because derivatives and swaps created by the exchange might be sold away from a "designated contract market" (*i.e.*, a CFTC-registered exchange) to persons who are not "eligible contract participants," which would violate the CEA if there were sufficient U.S. nexus (as would probably be the case).

to those of broker-dealers and clearing agencies -- or so the SEC has alleged in *Binance* and *Coinbase*.[127] An exchange that contracts to participate in the distribution of a token by, for example, allocating the token to accounts of its customers, might well be viewed as a distributor. Likewise, a trading firm that contracts to make a market in a token undergoing distribution might well be viewed as a distributor.

The presence of a distributor is not fatal to invocation of Regulation S, but it does have consequences. Distributors are subject to "offering restrictions" in Category 2 and Category 3 offerings under Rule 902(g), according to which each distributor must agree in writing that all offers and sales during the distribution compliance period shall be made only in accordance with Rule 903 or 904, pursuant to Securities Act registration or pursuant to an available exemption, and, in the case of an equity securities offering by a domestic issuer, not to engage in hedging unless in compliance with the Securities Act.

As applicable here, Rule 904 exempts offshore resales by persons other than the issuer, a distributor, and their affiliates, or any person acting for any of them. The Rule 904 requirements are an "offshore transaction," as defined; no "directed selling efforts" in the United States, as defined; and, in the case of a dealer or other person receiving remuneration for selling, not knowing that the offeree or buyer is a U.S. person and, if such dealer or other person knows that the purchaser is a dealer or other person receiving remuneration for selling, then the first such person must send the second person a notice stating that the securities may be offered or sold during the distribution compliance period only in accordance with Regulation S, pursuant to Securities Act registration or pursuant to an available exemption.

In Categories 2 and 3 in and under Rule 903, each distributor selling to a distributor, dealer or person receiving remuneration for selling also must send to the purchaser, during the distribution compliance period, a notice stating that the purchaser is subject to the same restrictions on offers and sales that apply to a distributor.

The "agreements in writing" can be obtained in contracts with exchanges, market makers and other actual or potential distributors. The requisite "notices" by distributors can be coded into the tokens or, in the author's view, can be delivered by exchanges to their customers on behalf of the issuer and distributors that are required to give the notice. These requirements, it bears emphasis, apply only during the distribution compliance period and only for Category 2 and 3 offerings. They do not apply to Category 1 offerings.

There is an additional "paperwork" requirement in Category 3 (only) that merits mention. In the case of a domestic issuer (only), the securities must "contain a legend to the effect that transfer is prohibited except in accordance with" Regulation S, pursuant to Securities Act registration or pursuant to an available exemption, and that hedging may not be conducted unless in compliance with the Securities Act. Reference to a "legend" harkens back to the pre-digital era in which these safe harbors were adopted.

---

[127] *See* Complaint, SEC v. Binance, No. 1:23-cv-01599 (D. D.C. June 5, 2023); SEC v. Coinbase, Inc., No. 1:23-cv-04738 (S.D.N.Y. June 6, 2023). This chapter does not address the merits of the SEC's cases against these exchanges, which depend in any event upon proving that the exchanges transacted in securities.

This requirement can be satisfied by including the required text in the token's code, where it should be featured prominently, as legends are meant to highlight important information. There may be other ways to deliver the message with the same effect as a legend placed on a stock certificate or bond.

Digital assets generally, and crypto assets in particular, are "bearer" financial instruments, as to which ownership is not registered or recorded on a ledger that would position the issuer or a transfer agent to deny ownership or stop transfer to a new owner. Instead, token ownership and transfer are recognized by the consensus mechanisms built into permission-less blockchains. Since the issuer cannot police transfers of bearer assets, Category 3 requires the implementation of "reasonable procedures" such as the legend mentioned in this paragraph to prevent transfers not made in accordance with Regulation S. Again, including the text prominently in the token's code should suffice, and there may be other "reasonable procedures" (such as notices from an exchange) that would have the same effect.

In view of all the complexities, however, it would seem to be safest and best simply to avoid Category 3 offerings when possible.

In that connection, it may be necessary to confront another classification question, which is this: Since the digital asset in question at an early stage of ecosystem development is presumptively a "security," is it an "equity security" or a "debt security"? The answer to this question has a Regulation S impact in that only "debt securities" can be offered under Category 2. "Equity securities" are ineligible for Category 2. They must instead be offered and sold under Category 1 or Category 3, each of which presents challenges of its own that addressed above.

It is possible for digital assets to be structured as equity securities by providing for dividends or other features of stock, such as the right to vote for members of a board of directors. But that is not how thoughtful developers and their counsel structure crypto assets. Instead, they avoid the hallmarks of "stock" or another equity security (or a "note," for that matter) in the course of devising what might be an "investment contract" but would be no other type of security.

Rule 902(a) defines "debt securities" to mean "any security other than an equity security as defined in Rule 405," as well as certain other types of securities not relevant here. Rule 405 defines "equity security" as "any stock or similar security" and any of about a dozen other kinds of securities, without mentioning investment contracts. The author's view is that investment contracts are not equity securities as defined in Rule 405, so they are debt securities as defined in Rule 902(a) for the purposes of Regulation S. On this view, crypto assets without the features of stock can be offered and sold under Category 2, with its 40-day distribution compliance period, rather than the more burdensome Category 3. The SEC has published no guidance either way. Some token issuers adopt the more conservative position and use Category 3.

Classification of a digital asset as an equity security would have other consequences under the U.S. federal securities laws. Most significantly, under Exchange Act Section 12(g), an issuer using U.S. jurisdictional means generally must register with the SEC

under the Exchange Act and begin to file periodic reports (such as Forms 10-K, 10-Q and 8-K) after it has total assets of at least $10 million and a class of equity security held of record by either 2,000 persons or by 500 persons that are not accredited investors. The vast majority of crypto asset projects would fit this description after a successful public sale of tokens under Regulation S, although the tokens would be bearer assets such that a reliable count of record holders could not be obtained.

These issues were addressed by the SEC Staff and by counsel to the issuer in connection with the Blockstack Token LLC offering proposed to be made in 2019 under SEC Regulation A. Blockstack initially took the position that its tokens were "investment contracts, and not debt or equity."[128] Later, it argued at length that its tokens were debt securities for purposes of Regulation A, and also for purposes of Rule 144, and were not equity securities for purposes of Section 12(g).[129] The issues were unresolved when Blockstack withdrew its Offering Statement on Form 1-A in order to pursue a Regulation A offering through an affiliate.[130]

An offering under Regulation S by a subsidiary of a foundation that has no shareholders is not riskless. In addition to the risks inherent in any exempt offering, there is the added risk that the SEC will attack because of its hostility toward crypto asset offerings in general and the uncertainties associated with the SEC's general refusal to give written guidance to blockchain technology entrepreneurs and their counsel. The SEC and its Staff have given no written guidance whatsoever to the digital asset industry relative to Regulation S.

A core concern is the risk of ex post litigation and possible findings of "control person" liability or "aiding and abetting" liability. On the first point, Securities Act Section 15(a) states that "[e]very person who, by or through stock ownership, agency, or otherwise, or who, pursuant to or in connection with an agreement or understanding with one or more other persons by or through stock ownership, agency, or otherwise, controls any person liable under sections [11] or [12] of this title, shall also be liable jointly and severally with and to the same extent as such controlled person to any person to whom such controlled person is liable, unless the controlling person had no

---

[128] *See* Letter from Robert H. Rosenblum, Attorney, Wilson Sonsini Goodrich & Rosati, to David Gessert, Staff Attorney, SEC (Dec. 21, 2018), https://www.sec.gov/Archives/edgar/data/1719379/000110465919020748/a18-15736_1ex1a15addexhbd5.htm (last visited July 27, 2023).

[129] *See* Letter from Robert H. Rosenblum, Attorney, Wilson Sonsini Goodrich & Rosati, to Sara von Althann, Staff Attorney, SEC (May 17, 2019), https://www.sec.gov/Archives/edgar/data/1725129/000162827919000230/exhibit155-1a.htm (last visited July 27, 2023). Blockstack's counsel observed in this letter that, if Blockstack became subject to Section 12(g) reporting requirements, then it "also would become subject to a large number of significant regulatory regimes that would make no sense as applied to Blockstack." These would include the proxy rules, the tender offer rules, the beneficial ownership reporting rules, and others. *Id.* at 9. And these rules would apply to any token issuer with more than 2,000 token holders and $10 million in assets, *regardless of whether it files under Regulation A*." *Id.* at 10 (emphasis in original).

[130] *See* Blockstack Token LLC, Withdrawal of Form 1-A (As Amended) (July 18, 2019); Blockstack PBC, Offering Circular (July 11, 2019).

knowledge of or reasonable ground to believe in the existence of the facts by reason of which the liability of the controlled person is alleged to exist." Section 15(b) states that "any person that knowingly or recklessly provides substantial assistance to another person in violation of a provision of this subchapter, or of any rule or regulation issued under this subchapter, shall be deemed to be in violation of such provision to the same extent as the person to whom such assistance is provided."

A well-designed and executed offering program that includes migration off-shore into a shareholder-less foundation managed by a Board of Directors controlled by persons unaffiliated with APs should obviate "control" within the meaning of Section 15(a) and should negate knowing or reckless "substantial assistance" within the meaning of Section 15(b). Also, in each case, there could be no secondary liability unless there were primary liability on the part of the foundation, a foundation subsidiary or other seller. Regulation S, if used correctly, provides a safe harbor from primary liability for a Securities Act registration violation. Therefore, the suggestions made in this chapter should result, if implemented, in no liability on the part of anyone for failure to register under the Securities Act.

Some token issuers have tried, but failed, to satisfy off-shore offering requirements. Of these, the Block.One SEC enforcement proceedings is perhaps the most notable precedent.[131] This was a $24 million settlement for Securities Act registration violations in an ICO effectuated between June 2017 and June 2018, through which Block.One raised about $4 billion, mostly outside the United States. "At the time the ICO launched in June 2017, Block.One did not have any product in place, and its proposed software was largely conceptual."[132] The ICO tokens were securities because purchasers "would have had a reasonable expectation of obtaining a future profit based upon Block.One's efforts, including its development of the EOSIO software and its promotion of the adoption and success of EOSIO and the launch of the anticipated EOSIO blockchains."[133]

Block.One sold its tokens in two tranches. The ICO tranche became non-transferable upon the ICO closing. The post-ICO tranche was transferable and could be used on the EOSIO blockchain that launched two weeks post-closing. The SEC's acceptance of the EOS token sales after the ICO closed and the EOS Blockchain launched was significant, in the author's view, because it implied that those tokens were not securities. They would have been non-security commodities due to sufficient decentralization or full functionality (or both).

The SEC's narrative concerning Block.One's Securities Act registration violation made three key points:

1. The EOS.IO Website included certain measures intended to block U.S.-based purchasers from buying ERC-20 Tokens, including by blocking U.S.-based IP

---

[131] *See* In re Block.One, SEC Release No. 33-10714 (Sept. 30, 2019).
[132] *Id.*
[133] *Id.*

> addresses from accessing the EOS.IO Website token sale page. In addition, Block.one required all ERC-20 Token purchasers to agree to the Token Purchase Agreement, which included provisions that U.S. persons were prohibited from purchasing ERC-20 Tokens, and that any purchase by a U.S. person was unlawful and rendered the purchase agreement null and vo*Id.* Block.one did not, however, ascertain from purchasers whether they were in fact U.S.-based persons, and a number of U.S.-based persons purchased ERC-20 Tokens directly through the EOS.IO Website.[134]

The lesson here is the need to verify the non-U.S. person status of purchasers. This chapter explains how that can be achieved.

2. Block.one also undertook efforts for the purpose of, or that could reasonably be expected to have the effect of, conditioning the market in the U.S. for the ERC-20 Tokens, including by engaging in directed selling efforts. Among other things, Block.one participated in blockchain conferences in the U.S. to promote Block.one and which at times also promoted its ICO. Block.one advertised EOSIO on a large billboard in Times Square, promoted EOSIO in informal informational sessions and hosted a post-conference reception. Block.one also promoted its proposed business and ICO to U.S.-based persons on the EOS.IO Website and through various social media and forum posts. The EOS.IO Website, White Paper, and other promotional statements were accessible to purchasers and potential purchasers, and viewable by U.S. persons.[135]

The lesson here is to avoid U.S. promotion, which is "directed selling efforts" as discussed in this chapter.

3. ERC-20 Tokens were traded and widely available for purchase on numerous online trading platforms open to U.S.-based purchasers throughout the duration of the ICO. Block.one did not take any steps to prevent the ERC-20 Tokens from being immediately resellable to U.S.-based purchasers in secondary market trades.[136]

The lesson here is to inhibit flowback during the immediate post-offering period. This chapter explains when and how to do that.[137]

There are other cases in which the SEC has pursued token issuers and their controlling persons. In these cases, at least in the SEC's telling, off-shore offering requirements were not satisfied.[138]

---

[134] *Id.* ¶ 10.
[135] *Id.* ¶ 11.
[136] *Id.* ¶ 12.
[137] See supra p. 21.
[138] *See, e.g.*, Order Instituting Cease-and-Desist Proceedings, *In re Blockchain Credit Partners*, Securities Act Release No. 10961, Exchange Act Release No. 92588 (Aug. 6, 2021) (settling with the entity and the individuals after finding that a Cayman Islands corporation—not a foundation—owned all the tokens when the currency was created and received the proceeds when they were sold; the parties engaged in fraudulent activity; and the parties marketed the tokens through considerable use of social media, the parties did not attempt to comply with Regulation S—"the DMM website was publicly available and was

K. Disclosure Recommendations

Under existing law, the disclosure surrounding an offering exempt from Securities Act registration by reason of Regulation S or the private offering exemption is free writing, which is to say that no particular disclosure is required. Avoiding the various species of fraud is sufficient. In general, that means avoidance of statements that are materially false or misleading.

This is an area that is overdue for guidance. The SEC does not characteristically provide guidance on disclosure issues, expecting issuers and others with disclosure obligations to determine for themselves, ideally with assistance from experienced disclosure counsel, what should be disclosed in an exempt offering. Classically, disclosure is provided on the same three broad topic areas that registered offerings also cover. These are: disclosure about the issuer, particularly its business, management and financials; disclosure about the security being offered; and disclosure about the market for the security, including the manner of offering or plan of distribution.

Logically, an exempt offering of digital assets should cover the same general topics, modified to reflect the realities of the digital assets industry and the token economy. Disclosure that would be prescribed for a conventional business is both overinclusive and underinclusive of sound disclosure for a token offering. This is especially so once the protocol and token have become sufficiently decentralized: What disclosure about management makes sense for something that has no management? None.

Capitol Hill seems to understand this point. Both the House bill and the Senate bill that are currently pending call for disclosure that reflects the unique features and risks of the digital assets industry and the token economy.

While the pending bills are meant to cover offerings that might or might not be regulated by the SEC, they are nonetheless informative about the topics that should be covered in an SEC-exempt offering such as a Regulation S or private offering. So, here the disclosure requirements of the leading bipartisan Senate bill[139] and House bill[140] will

---

at no time password-protected or geographically restricted"); Complaint, SEC v. Rivetz Corp., No. 3:21-cv-30092 (D. Mass Sept. 8, 2021) (alleging that the parties used a Cayman Islands entity, but badly; the Cayman Islands company was a wholly-owned subsidiary of the Delaware corporation that defendant controlled as a 40% shareholder and CEO, and he was a director of the Cayman Islands company; the Delaware corporation advertised on website and via social media that tokens could be bought from the Cayman Islands entity by U.S. persons and globally; the individual defendant was as a direct violator of Section 5; and that "each defendant directly and/or indirectly offered and sold securities without a registration statement in effect, engaged in steps necessary to the public distribution of unregistered securities, and was a necessary participant in the offering of unregistered securities").

[139] See Lummis-Gillibrand Responsible Financial Innovation Act of 2023, 118th Cong. 1st Sess., https://tinyurl.com/4azn9fkp ("Lummis-Gillibrand"). The Lummis-Gillibrand section-by-section overview is available at https://tinyurl.com/4z995fvm. As its name reflects, Sen. Cynthia Lummis (R-WY) and Sen. Kirsten Gillibrand (D-NY) champion this bill.

[140] See H.R. 4763, Financial Innovation and Technology for the 21st Century Act, as submitted to July 26, 2023 mark-up, https://tinyurl.com/3hz7c4j9 (the "FIT Act"). A section-by-section summary of the FIT Act is available at https://tinyurl.com/yxb3ybtb. House Financial Services Committee Chairman Patrick

be presented. Pending adoption into law, they should be considered guideposts or checklists for the preparation of high-quality disclosure and benchmarks against which the quality of disclosure can be judged.

Of the Senate bill and the House bill, the former is rather more elaborate than the latter on disclosure. The Senate bill does not specify disclosure requirements for a primary offering of tokens but does provide detailed requirements for semiannual disclosure, akin to SEC reporting requirements for public companies. The requirements are as follows:[141]

> (1) Basic corporate information regarding the issuer, including the following:
>
> (A) The experience of the issuer in developing assets similar to the ancillary asset.[142]
>
> (B) If the issuer has previously provided ancillary assets to purchasers of securities, information on the subsequent history of those previously provided ancillary assets, including price history, if the information is publicly available.
>
> (C) The activities that the issuer has taken in the relevant disclosure period, and is projecting to take in the 1-year period following the submission of the disclosure, with respect to promoting the use, value, or resale of the ancillary asset (including any activity to facilitate the creation or maintenance of a trading market for the ancillary asset and any network or system that utilizes the ancillary asset).
>
> (D) The anticipated cost of the activities of the issuer in subparagraph (C) and whether the issuer has unencumbered, liquid funds equal to that amount.
>
> (E) To the extent the ancillary asset involves the use of a particular technology, the experience of the issuer with the use of that technology.

McHenry (R-NC) and Subcommittee on Digital Assets, Financial Technology and Inclusion Chairman French Hill (R-AK) champion the FIT Act, which passed the House Financial Services Committee on July 26, 2023 with bipartisan support. See Press Release, House Financial Services Committee Reports Digital Asset Market Structure, National Security Legislation to Full House for Consideration, July 26, 023, https://tinyurl.com/3jmbr2x9. The legislation has not moved since then, perhaps because of the emergence of higher priorities such as the federal debt and the wars in Ukraine and the Mideast.

[141] The disclosure items listed in the text are drawn from Section 501(c) of Lummis-Gillibrand.

[142] The term "ancillary asset" is a core concept in Lummis-Gillibrand. It is defined by Section 501(a)(1) of the bill as "an intangible, fungible asset that is offered, sold, or otherwise provided to a person in connection with the purchase and sale of a security through an arrangement or scheme that constitutes an investment contract, as that term is used in section 2(a)(1) of the Securities Act," excluding an asset that provides the holder a debt or equity interest in a business entity, liquidation rights with respect to a business entity, an entitlement to an interest payment or dividend payment from business entity or any other financial interest in a business entity. In other words, an ancillary asset is a *Howey* investment contract, excluding (for avoidance of doubt) debt, equity, liquidation, interest and dividend rights and other financial interests in business entities.

(F) The backgrounds of the board of directors (or equivalent body), senior management, and key employees of the issuer, the experience or functions of whom are material to the value of the ancillary asset, as well as any personnel changes relating to the issuer during the period covered by the disclosure.

(G) A description of the assets and liabilities of the issuer, to the extent material to the value of the ancillary asset.

(H) A description of any legal proceedings in which the issuer is engaged (including inquiries by governmental agencies into the activities of the issuer), to the extent material to the value of the ancillary asset.

(I) Risk factors relating to the impact of the issuer on, or unique knowledge relating to, the value of the ancillary asset.

(J) Information relating to ownership of the ancillary asset by—

(i) persons owning not less than 10 percent of any class of equity security of the issuer; and

(ii) the management of the issuer.

(K) Information relating to transactions involving the ancillary asset by the issuer with related persons, promoters, and control persons.

(L) Recent sales or similar dispositions of ancillary assets by the issuer and affiliates of the issuer.

(M) Purchases or similar dispositions of ancillary assets by the issuer and affiliates of the issuer.

(N) A going concern statement from the chief financial officer of the issuer or equivalent official, signed under penalty of perjury, stating whether the issuer maintains the financial resources to continue business as a going concern for the 1-year period following the submission of the disclosure, absent a material change in circumstances.

(2) Information relating to the ancillary asset, including the following:

(A) A general description of the ancillary asset, including the standard unit of measure with respect to the ancillary asset, the intended or known functionality and uses of the ancillary asset, the market for the ancillary asset, other assets or services that may compete with the ancillary asset, and the total supply of the ancillary asset or the manner and rate of the ongoing production or creation of the ancillary asset.

(B) If ancillary assets have been offered, sold, or otherwise provided by the issuer to investors, intermediaries, or resellers, a description of the amount of assets offered, sold, or provided, the terms of each such transaction, and any contractual or other restrictions on the resale of the assets by intermediaries.

(C) If ancillary assets were distributed without charge, a description of each distribution, including the identity of any recipient that received more than 5 percent of the total amount of the ancillary assets in any such distribution.

(D) The amount of ancillary assets owned by the issuer.

(E) For the 1-year period following the submission of the disclosure, a description of the plans of the issuer to support (or to cease supporting) the use or development of the ancillary asset, including markets for the ancillary asset and each platform or system that uses the ancillary asset.

(F) Each third party not affiliated with the issuer, the activities of which may have a material impact on the value of the ancillary asset.

(G) Risk factors known to the issuer that may limit demand for, or interest in, the ancillary asset.

(H) The names and locations of the markets in which the ancillary asset is known by the issuer to be available for sale or purchase.

(I) To the extent available to the issuer, the average daily price for a constant unit of value of the ancillary asset during the relevant reporting period, as well as the 12-month high and low prices for the ancillary asset.

(J) If applicable, information relating to any external audit of the code and functionality of the ancillary asset, including the entity performing the audit and the experience of the entity in conducting similar audits.

(K) If applicable, any third-party valuation report or economic analysis regarding the ancillary asset or the projected market of the ancillary asset, which shall include the entity performing the valuation or analysis and the experience of the entity in conducting similar reports or analyses.

(L) If the ancillary asset is intangible, information relating to custody by the owner of the ancillary asset or a third party.

(M) Information on intellectual property rights claimed or disputed relating to the ancillary asset.

(N) A description of the technology underlying the ancillary asset.

(O) Any material tax considerations applicable to owning, storing, using, or trading the ancillary asset.

(P) Any material legal or regulatory considerations applicable to owning, storing, using, or trading the ancillary asset, including any legal proceeding that may impact the value of the ancillary asset.

(Q) Any other material factor or information that may impact the value of the ancillary asset and about which the issuer is reasonably aware.

These digital asset disclosure topics resemble traditional disclosure topics in their focus on the business of the issuer, the features of the token and the markets in which the token is sold. They arguably exceed traditional disclosure mandates by requiring, for example, a going concern statement and information relating to any external audit of the code and functionality of the ancillary asset and any third-party valuation report or economic analysis regarding the ancillary asset or its projected market. The collection of requirements is sensible, considering the context. Of particular note is the very last listed topic – "any other material factor or information" of which the issuer "is reasonably aware" – which resembles the venerable antifraud standards adopted by Congress and the SEC in the securities laws.

The Lummis-Gillibrand section-by-section overview assets that "Lummis-Gillibrand strengthens our existing laws requiring tailored disclosures relating to ancillary assets, ensuring consumers have the information they need to make informed financial decisions." That seems correct as a matter of law and policy. And again, while the bill requires these disclosures twice a year for ancillary assets (which are investment contracts or other securities), the same topics might advisably be viewed as disclosure guides in the primary offering of the same assets. Furthermore, it would be useful to the public (though efficiency would be lost, and cost recovery might not be assured) if some proxy for the issuer – the Lab, perchance, or a centralized exchange, listing the token – were to disclose at least some of this information to the market for mutated tokens (that no longer are securities).[143]

The House bill, in contrast to the Senate bill, requires disclosure on only six topics. Specifically, with respect to a digital asset and its associated blockchain system, Section 203(a) of the FIT Act requires disclosure regarding:

(1) SOURCE CODE —The source code for any blockchain system to which the digital asset relates.

(2) TRANSACTION HISTORY —The steps necessary to independently access, search and verify the transaction history of the related blockchain system.

(3) TOKENOMICS —The purpose and the operation of the related blockchain system, including—

(A) information explaining the launch and supply process, including the number of digital assets to be issued in an initial allocation, the total number of digital assets to be created, the release schedule for the digital assets, and the total number of digital assets then outstanding;

(B) information on any applicable consensus mechanism or process for validating transactions, method of generating or mining digital assets, and any process for burning or destroying digital assets on the blockchain system;

[143] Lummis-Gillibrand also anticipates plain language disclosure to customers regarding ancillary assets to customers. Section 204(b) of the bill would require the SEC, in consultation with the CFPB, to issue "best practices" guidance for issuers regarding two-page plain language summaries about the ancillary assets, to be filed with the SEC.

(C) an explanation of governance mechanisms for implementing changes to the blockchain system or forming consensus among holders of such digital assets; and
(D) sufficient information for a third party to create a tool for verifying the transaction history of the digital asset.
(4) PLAN OF DEVELOPMENT — The current state and timeline for the development of the related blockchain system, showing how and when that system intends or is intended to be considered a functional network and decentralized network.
(5) DEVELOPMENT DISCLOSURES — A list of all persons who are related persons or affiliated persons who have been issued a unit of a digital asset by a digital asset issuer or have a right to a unit of a digital asset from a digital asset issuer.
(6) RISK FACTORS — Where appropriate, under the caption "Risk Factors," the material risks surrounding ownership of a unit of the digital asset. This discussion is to be organized logically with relevant headings, with each risk factor set forth under a sub-caption that adequately describes the risk.

As provided in Section 203(b) of the FIT Act, the required information need not be made available by the issuer but may instead be certified by an affiliated person (such as the Lab), a decentralized governance system (*i.e.*, a DAO) or an exchange.

The proposed FIT Act offers a lighter touch on required disclosure than Lummis-Gillibrand, but is not for that reason deficient. The emphasis on tokenomics and plan of development, and risk factors of course, are especially wholesome. That information is hard to find from reliable sources in the case of many tokens in the market today.

The House bill and the Senate bill both serve valuable disclosure guidance purposes even though neither one has been enacted into law yet.

L. After the Regulation S Offering

The ultimate question is the status of the protocol and the token after the Regulation S offering has closed and any distribution compliance period has expired. At a minimum, the tokens remain investment contracts, and therefore securities, but they were sold in compliance with a Securities Act registration exemption—Regulation S—and can be resold under another Securities Act registration exemption. They will not be treated as "restricted securities" under SEC Rule 144 because they are not equity securities of a domestic issuer.[144] Instead, they are probably debt securities and, even if not, their issuer is a foreign issuer. They can be resold under Securities Act Section 4(a)(1) in transactions by any person other than an issuer, underwriter or dealer.[145]

At a maximum—and this is the objective—after the Regulation S offering, including any distribution compliance period (or other lock-up), the tokens have mutated into non-security commodities. As such, they can be resold without any consideration of the U.S. federal securities laws. This is more easily said than done. When it happens,

[144] *See* 17 C.F.R. § 230.144(a)(3)(v).
[145] *See* 15 U.S.C. § 77d(a)(1).

though, it will be the product of careful planning and execution by the Lab, its legal counsel and others over a year or longer (possibly several years).

Saying that the tokens have "mutated" means that the protocol and token have become "sufficiently decentralized" in the "When Howey Met Gary (Plastic)" and FinHub Framework sense. They have become non-security commodities because they fail the "efforts of others" prong of *Howey*. This requires that the elements of sufficient decentralization have been satisfied. Without discussing that topic exhaustively in this chapter, the following facts and circumstances should be extant for sufficient decentralization to be in effect:

- The tokens are broadly held by persons having little or no relationship with one another, ideally located on multiple continents;
- Improvements in the protocol and token are effectuated by a formal or informal DAO whose members may include, but not be driven by, APs;
- The foundation is governed by a board, a majority of whose members are independent of the APs, and by a steward or stewards who are likewise independent; and
- The APs play no significant entrepreneurial or managerial role in the operation and planned growth of the ecosystem; whatever role they do play could be performed equally well by others; in short, the protocol and protocol and token pass the Bahamas test.

Alternatively, the protocol and token are fully functional in the "When Howey Met Gary (Plastic)" and FinHub Framework sense. They have mutated and are now non-security commodities because they fail the "expectation of profits" prong of *Howey*. It is possible that some persons purchase tokens for investment, but the primary motivation for purchase is consumption. Obviously, goods or services must be available for purchase in the ecosystem.

There is some precedent for the view that token holders cannot be expecting APs to continue to build or improve the ecosystem, as in that case they are continuing to rely upon others to produce a profit.[146] The author rejects that district court decision as a misinterpretation of the "expectation of profits" prong of Howey as explained in *Forman*. It should be enough that the motivation primarily is consumption. Otherwise, the purchase of goods by any consumer products company would be a securities transaction if the goods could be resold and if the company were known to be committed to improving the customer experience.

Ideally, both conditions are satisfied when the Regulation S offering has closed and any distribution compliance period or other lock-up has expired: sufficient decentralization and full functionality. The classic examples of this are the characteristics of BTC and ETH in 2019.

---

[146] *See, e.g.*, SEC v. LBRY, Inc., 2022 WL 356772 (D. N.H. 2022) (No. 21-cv-260-PB).

It is instead possible, however, that neither condition will have been satisfied when the Regulation S lock-up is due to expire. In that case, it is best to extend the lock-up until one or both conditions are satisfied, although this might disappoint token purchasers. Alternatively, the tokens can be allowed to trade free of restrictions, in which case they will be exempt from Securities Act registration, as noted earlier. But in that case no other or additional offering should be made until one or both conditions can be satisfied, except pursuant to an exemption (such as Regulation D or Regulation S) or registration.

As a matter of good governance, decisions about mutation from security status to non-security status should be made by the foundation's board, acting upon advice of counsel and in close consultation with counsel who are expert in such matters.[147]

[147] The management of Hiro Systems PBC ('Hiro') concluded that, as Stacks Blockchain 2.0 has been adopted by the Stacks mining community, Hiro is no longer in the position of providing, and will no longer be able to provide, essential managerial services to the Stacks Blockchain. Management concluded further that if Hiro is no longer in the position of providing, and will no longer be able to provide, essential managerial services to the Stacks Blockchain, then it is no longer necessary for Hiro to treat the Stacks Tokens as investment contracts that are securities under the federal securities laws. The management of Hiro presented these conclusions to the Board of Directors of Hiro (the 'Board'), and on January 20, 2021, the Board voted to approve the decision of management to no longer treat the Stacks Tokens as investment contracts that are securities under the federal securities laws.
Hiro Systems PBC, Current Report (Form 1-U) (Jan. 20, 2021); *see* also Hiro Systems PBC, Current Report (Form 1-U) (Dec. 7, 2020) (disclosing the release of a summary of a memorandum prepared for Blockstack's board by legal counsel with factual input from Blockstack); Rosenblum, Caiazza & Collins-Wood, *supra* note 93.

Centralized Exchanges

Bill Martin and Scott Sugino*

A. Introduction

A centralized exchange (CEX) is an organized marketplace that facilitates the trading of digital assets. As discussed in this chapter, CEXs are designed to function as trusted intermediaries, which provide users with access to digital assets, liquidity to support trading those assets, and custodial services in a secure and centralized environment. Like centralized exchanges for stocks or other traditional assets, CEXs offer asset standardization, peer-to-peer trading, firm bids and offers, and price transparency. These features are what make CEX platforms attractive to both experienced traders and newcomers to crypto. CEXs are critical players in today's crypto industry.[1]

While there are hundreds of CEXs around the world, today's largest, by trading volume, are Binance.com, Coinbase, and Kraken.[2] These platforms have brought crypto into the mainstream through innovative and easy-to-use interfaces, but some have also drawn scrutiny from the SEC and are now engaged in ongoing litigation.

1. U.S. CEXs

Binance.US: Binance.US enabled users to convert fiat into cryptocurrencies and trade them, while also allowing users to store their digital assets in a Binance.US wallet.[3] In June 2023, Binance.US transitioned into a crypto-only exchange, which means

---

* Martin is Counsel at O'Melveny in New York, NY (https://www.omm.com/professionals/william-j-martin/); Sugino is a Partner at O'Melveny in Los Angeles, CA (see https://www.omm.com/professionals/scott-sugino/). Carl Fornaris, Partner at Winston & Strawn LLP, reviewed this chapter.

[1] KPMG, *Crypto Insights Part 2: Decentralised Exchanges and Automated Market Makers*, (October 2021), https://assets.kpmg.com/content/dam/kpmg/cn/pdf/en/2021/10/crypto-insights-part-2-decentralised-exchanges-and-automated-market-makers.pdf.

[2] CoinMarketCap, *Exchange Rankings*, https://coinmarketcap.com/rankings/exchanges/.

[3] Binance Support, *A Complete Guide To Using Binance.US as a Crypto-Only Exchange*, https://support.binance.us/hc/en-us/articles/15259026846487-A-Complete-Guide-To-Using-Binance-US-as-a-Crypto-Only-Exchange#h_01H4P9W178GACC14Z48HC03907 (September 2023).

they do not accept USD deposits or withdrawals.[4] On June 5, 2023, the Securities and Exchange Commission (SEC) accused Binance entities of violating U.S securities laws, including (i) operating as an unregistered securities exchange, broker, and clearing agency; (ii) offering and selling unregistered crypto assets; (iii) failing to restrict U.S. investors from accessing Binance.com; (iv) misleading investors; and (v) mishandling customer funds.[5] The court partially granted Binance's motion to dismiss the SEC's claims concerning secondary sales, but it denied the motion as to certain token offerings, staking services, the failure to register, and fraud. The suit is ongoing.

Coinbase: Coinbase enables individuals to trade cryptocurrencies and facilitates borrowing for those trades. Coinbase also offers a wallet service that allows users to store their digital assets. On June 6, 2023, the SEC charged Coinbase with operating its crypto asset trading platform as an unregistered national securities exchange, broker, and clearing agency,[6] and with offering unregistered securities on its platform.[7] Coinbase denied the allegations and filed a motion for judgment on the pleadings in August, arguing, among other things, that the SEC's complaint violates due process and that the subject is outside the SEC's delegated authority. The court denied Coinbase's motion for judgment on the pleadings, except to the extent the SEC's claim concerns Coinbase's wallet product.

Kraken: Users can trade digital assets and futures, with the use of margin, on Kraken, which also offers a custodial wallet for digital assets, including non-fungible tokens (NFTs).[8] Kraken used to operate a digital asset staking business, but in early 2023, it agreed to shut it down in a settlement with the SEC. Kraken also previously paid a fine for violating U.S economic sanctions.

OpenSea: The world's first and largest web3 marketplace for NFTs and crypto collectibles, OpenSea allows for the direct sale of NFTs at a fixed price or through an auction.[9] OpenSea has been subject to several lawsuits due to a flaw in its system that allowed hackers to steal NFTs or purchase them for less than the asking price.[10] One individual filed suit in the Southern District of Texas, alleging that a hacker exploited an OpenSea security vulnerability to access his wallet and list and sell his NFT for a fraction of its value.[11] The parties were ordered to arbitration on March 22, 2023.

---

[4] *Id.*
[5] Matthew Goldstein, Emily Flitter and David Yaffe-Bellany, *SEC Brings Charges Against Binance*, The N.Y. TIMES (June 5, 2023), https://www.nytimes.com/2023/06/05/business/sec-binance-charges.html.
[6] Press Release, U.S. Securities and Exchange Commission, Press Release, SEC Charges Binance with Violating Securities Laws, (June 13, 2023), https://www.sec.gov/news/press-release/2023-102.
[7] *Id.*
[8] Kraken, https://www.kraken.com/
[9] OpenSea, *About OpenSea*, https://opensea.io/about.
[10] David Yaffe-Bellany, *Lawsuits Against OpenSea Amid Cryptocurrency Price Crash,* THE N.Y. TIMES (June 6, 2022), https://www.nytimes.com/2022/06/06/technology/nft-opensea-theft-fraud.html#:~:text=The%20company%20is%20facing%20at%20least%20four%20lawsuits,NFTs%20cool.
[11] Complaint, *McKimmy v. Opensea*, No. 4:22-cv-00545 (S.D. Tx, 2022), https://ia802202.us.archive.org/11/items/1-main_202202/1-main.pdf.

BitMEX: BitMEX is a CEX and derivative trading platform.[12] In August 2021, a federal court entered a consent order in which BitMEX agreed to pay a $100 million penalty for illegally operating a cryptocurrency trading platform and anti-money laundering violations.[13] At the same time, the U.S. Attorney's Office for the Southern District of New York indicted BitMEX founders Arthur Hayes, Benjamin Delo, and Samuel Reed on charges of willfully causing BitMEX to violate the Bank Secrecy Act and conspiracy to commit that offense.[14] All three founders pled guilty to violating the Bank Secrecy Act at varying points in February and March 2022.[15]

2. International CEXs

Binance.com: Not to be confused with Binance.US, Binance.com is a Malta-registered CEX founded in 2017.[16] It was initially based in China, but moved its headquarters in response to regulatory actions by the Chinese government.[17] Binance.com quickly became one of the largest and most well-known cryptocurrency exchanges—by 2018, it was the world's largest CEX and it retained that title through 2021.[18] The company has also launched two cryptocurrencies which it developed—Binance Coin (BNB) and BinanceUSD (BUSD).[19] Binance.com is now blocked for U.S.-based users.[20]

KuCoin: A Seychelles-registered CEX founded in 2017, KuCoin is a full-featured spot trading platform.[21] KuCoin used its own cryptocurrency, KuCoin Shares (KCS), to fund the creation of the exchange.[22] KuCoin offers customers a variety of futures, staking, and lending programs, including KuCoin Lend and proof-of-stake mining

---

[12] BitMEX, Why BitMEX, https://www.bitmex.com/why-bitmex.x
[13] Press Release, U.S. Commodity Futures Trading Commission, Federal Court Orders BitMEX to Pay $100 Million for Illegally Operating a Cryptocurrency Trading Platform and Anti-Money Laundering Violations, (August 10, 2021), https://www.cftc.gov/PressRoom/PressReleases/8412-21. 1
[14] *Id.*
[15] Press Release, Department of Justice, Third Founder of Cryptocurrency Exchange Pleads Guilty to Bank Secrecy Act Violations, (March 9, 2022), https://www.justice.gov/usao-sdny/pr/third-founder-cryptocurrency-exchange-pleads-guilty-bank-secrecy-act-violations.
[16] Yuji Nakamura, *World's Biggest CryptoCurrency Exchange is Heading to Malta,* BLOOMBERG (March 23, 2018), https://www.bloomberg.com/news/articles/2018-03-23/the-world-s-biggest-cryptocurrency-exchange-is-moving-to-malta.
[17] Eva Xiao, *Three Months After Launch, This Unbanked Crypto Exchange Made $7.5m in Profit,* TECH IN ASIA (November 30, 2017), https://www.techinasia.com/cryptocurrency-exchange-binance.
[18] Michael J. de la Merced and Jason Karaian, *What's Next for Coinbase,* N.Y. TIMES (April 15, 2021), https://www.nytimes.com/2021/04/15/business/coinbase-market-debut.html.
[19] Anneken Tappe, *Bitcoin? Ethereum? Dogecoin? Your guide to the biggest names in crypto*, CNN (April 22, 2021), https://www.cnn.com/2021/04/22/investing/cryptocurrency-guide-top-five-bitcoin-ethereum/index.html.
[20] Binance, https://www.binance.com/en.
[21] IQ.wiki, *KuCoin*, https://iq.wiki/wiki/kucoin.
[22] *Id.*

pools.[23] KuCoin is not licensed to operate in the U.S. and access to the platform is blocked for U.S. citizens and residents.

Bitfinex: Registered in the British Virgin Islands, this CEX began as a margin lending platform for Bitcoin only and over time has added other crypto assets, currently supporting more than 170.[24] Bitfinex provides exchange, margin, and derivatives trading, margin funding, and OTC markets. It has been subject to a number of regulatory challenges, including fines from the Commodity Futures Trading Commission (CFTC) and the New York Attorney General over statements about its reserves and losses relating to the stablecoin Tether. The Bitfinex platform is blocked for U.S. citizens and residents.

3. Types of CEXs

While CEXs vary widely in the products and services they offer, they usually share a number of characteristics, many of which appeal to a wide range of consumers—especially customers new to the cryptocurrency space.[25]

Generally, CEXs have a common infrastructure, including a matching engine, user interface, system for recording transactions, and information security. Many of the trades on these platforms occur internally, on the platform's systems, and not on the blockchain. Users can access the platforms through internet browsers or phone applications, and users logging into any CEX interface can expect to find a similar layout, easily navigated, which allows a user to trade on the blockchain without having to actually understand blockchain technology. Matching trade orders on a CEX requires several steps, including order placement, maintenance of an order book, matching engine, trade execution, and settlement. Customers typically place buy or sell orders, specifying the asset, quantity, and desired price. A matching engine continuously compares buy and sell orders placed by customers. Once there's a match, the CEX executes the trade and reflects the changes in ownership and balances from each account. CEXs are essential for providing liquidity, efficient price discovery, and ease of trading for customers.

4. Other Types of Exchanges

Although this chapter only addresses CEXs, there are other types of digital asset exchanges, and some may overlap with CEXs. Among them are decentralized

---

[23] *Id.*

[24] Eric Rosenberg, *Bitfinex Review,* INVESTOPEDIA (March 21, 2023), https://www.investopedia.com/bitfinex-review-5213318.

[25] Benedict George & Toby Bochan, *Centralized Exchange (CEX) v. Decentralized Exchange (DEX): What's the Difference?*, COINDESK (April 9, 2024), https://www.coindesk.com/learn/centralized-exchange-cex-vs-decentralized-exchange-dex-whats-the-difference/.

Exchanges (DEXs). DEXs have risen to prominence in recent years. As the name suggests, DEXs facilitate cryptocurrency transactions between two individuals directly.[26] They remove the need for a centralized entity, something the market has been intrigued with following the FTX saga,[27] and other high profile CEX cases.[28] Further, DEXs charge considerably less to process transactions (0.05% of the amount traded compared to Binance's 0.1% and Coinbase's 0.2%).[29] CEXs still dominate the exchange marketplace, with nearly 95% of exchange crypto trading taking place on CEXs.[30]

5. Types of Transactions

Exchanges offer trading and custodial services of different types of digital assets. Some CEXs facilitate spot transactions and others facilitate trading of derivatives; some, like Kraken and Binance, facilitate both. These types of transactions are explained below:

- **Spot Trading**. These transactions entail the immediate exchange of assets at a specified price and time.[31] Unlike most trades on traditional exchanges, which usually take time to settle after the contract is entered, cryptocurrency spot trades are settled the same day or nearly instantaneously.[32] CEXs achieve this through settling trades off-chain by recording transactions within their internal databases rather than directly on the blockchain.[33] When a customer places an order, the CEX matches it with another customer's complementary order, and the trade is executed off the blockchain.[34] The exchange then updates the

---

[26] *What are decentralized exchanges, and how do DEXs work*?, COINTELEGRAPH, https://cointelegraph.com/learn/what-are-decentralized-exchanges-and-how-do-dexs-work.
[27] Sage D. Young and Bradley Keoun, The Epic Collapse of Sam Bankman-Fried's FTX Exchange: A Crypto Markets Timeline, https://www.coindesk.com/markets/2022/11/12/the-epic-collapse-of-sam-bankman-frieds-ftx-exchange-a-crypto-markets-timeline/.
[28] Kyle Torpey, *Binance to Pay $4.3 Billion to Settle Criminal Charges as CEO Pleads Guilty, Steps Down,* INVESTOPEDIA (November 21, 2023), https://www.investopedia.com/crypto-exchange-binance-charged-with-money-laundering-fined-usd4-3-billion-8405545; Peter Whoriskey and Dalton Bennett, *Crypto's Free-Wheeling Firms Lured Millions. FTX Revealed the Dangers,* WASHINGTON POST (November 16, 2022), https://www.washingtonpost.com/business/2022/11/16/ftx-collapse-crypto-exchanges-regulation/.
[29] See George & Bochan, *supra* note 25.
[30] Benedict George, *What is a CEX? Centralized Exchanges Explained,* COINDESK (May 11, 2023), https://www.coindesk.com/learn/what-is-a-cex-centralized-exchanges-explained/.
[31] James Chen, *What is Spot Trading and How Do You Profit? How it Works,* (April 05, 2022), https://www.investopedia.com/terms/s/spottrade.asp.
[32] Onkar Singh, *What is Spot Trading in Crypto and How does it Work,* COINTELEGRAPH (December 10, 2022), https://cointelegraph.com/news/what-is-spot-trading-in-crypto-and-how-does-it-work.
[33] Jake Frankenfield, *Off-Chain Transactions: Definition, Advantages Vs. On-Chain,* INVESTOPEDIA (August 18, 2023), https://www.investopedia.com/terms/o/offchain-transactions-cryptocurrency.asp.
[34] Akash Kumar Jha, *Cryptocurrency Exchanges: Types, Comparison and Choosing the Right One for Trading?,* https://www.linkedin.com/pulse/cryptocurrency-exchanges-types-comparison-choosing-right-kumar-jha/.

customers' account balances within its internal ledger and later finalizes the settlement on the blockchain by executing an on-chain transaction to reflect the changes. This optimizes speed by reducing the overall network congestion and lowers fees associated with on-chain settlements.[35]

- **Derivative Trading**. Derivatives can be formed as contracts based on the price or future price of an underlying digital asset, but they do not involve the exchange of the underlying asset itself.

  Example: Derivative trading can involve complex products, but here is a relatively simple trade: When entering an order in a CEX to buy a Bitcoin future, the buyer is not buying actual BTC, but rather a contract related to the future price of BTC. The bitcoin future contract allows the buyer to sell BTC later at the price contracted earlier.

- **Margin Trading**. Some CEXs offer the opportunity to trade on margin, allowing customers to engage in spot or derivative trading with several times leverage.[36]

  Example: Customers can borrow funds from the CEX to trade larger positions than the customer's capital would allow. For instance, with $1,000 and 5x leverage, a customer could control $5,000 worth of a crypto currency. In this example, if the customer buys 50 units of a cryptocurrency at $100 each, with $1,000 of their own funds and $4,000 borrowed, and sells them later at $120 each, they would make a profit of $960 after repaying the borrowed amount and fees. However, if the trade goes against them, losses could exceed their initial deposit. Margin trading demands careful risk assessment.

6. Distribution of Digital Assets

Some CEXs have developed processes for identifying and evaluating digital assets before they list them on their platforms.[37] A CEX may require, for example, the project team that created the digital asset to submit general and economic information, a legal review, security audits, liquidity requirements, and more.[38] The CEXs generally consider technical requirements, and regulatory and business factors. Listing is typically seen as an expression of trust in a project by a CEX and an indication that there is sufficient liquidity in the associated asset.

---

[35] *Id.*; see Frankenfield, *supra* note 34.
[36] *See, e.g., Kraken*, https://www.kraken.com/features/margin-trading; Binance https://www.binance.com/en/trade/BTC_USDT?theme=dark&type=isolated.
[37] *See e.g.*, Suroj Chatterjee, *Listing Assets on Coinbase is Free and Always Has Been,* (May 31, 2022), https://www.coinbase.com/blog/listing-assets-on-coinbase-is-free-and-always-has-been.
[38] *How to Get Token Listed on Exchanges? | Step by Step Guide,* (December 1, 2022), https://gravityteam.co/blog/how-to-get-token-listed-on-exchange/.

- **Initial Exchange Offerings (IEOs).** CEXs can also facilitate IEOs, which were introduced in 2019 as an innovation on Initial Coin Offerings (ICOs).[39] IEOs serve the same capital-raising purpose as ICOs, but an IEO occurs through a centralized exchange that is responsible for the distribution and sale of the newly offered digital asset.[40] In exchange for facilitating the offer, the CEX is compensated by the issuer of the new asset.[41] After the IEO, the digital asset is listed on the CEX and available for trading.
- **Simple Agreement for Future Tokens (SAFT).** Crypto creators can also offer accredited investors contracts for future tokens. These contracts, called SAFTs, allow developers to receive investment for their new token; in exchange, the investors will receive the token at a discount at a later date.[42] SEC rules usually allow only accredited investors to enter into these contracts with the crypto creators in order to qualify for registration exemptions.
- **Airdrops.** When crypto developers give free tokens to people to encourage them to adopt a new token, it is called an airdrop.[43] In this marketing scheme, users can become part of the group that will receive the airdrop by completing certain tasks, such as following the developer's account on social media or spreading the word about the new token.[44]

7. CEX Users

One notable characteristic of CEXs is their availability to a wide range of customers.

Retail Investor Offerings. Individual retail investors are typically non-professionals who trade crypto through exchanges.[45] The most common services offered by major CEXs to individuals are trading—facilitating the buying and selling of cryptocurrency—and digital wallets, which allow secure custody of crypto holdings.[46] Beyond those, though, there are myriad offerings. For example, CEXs not only offer users the ability to

---

[39] Cryptopedia Staff, *IEOs and IDOs: An Evolution in Crypto Fundraising*, CRYPTOPEDIA (October 21, 2021), https://www.gemini.com/cryptopedia/ieo-crypto-ido-crypto-initial-exchange-offering#section-the-rise-of-initial-exchange-offerings.
[40] *Id.*
[41] *Id.*
[42] *Simple Agreement for Future Tokens (SAFT)*, CORPORATE FINANCE INSTITUTE, https://corporatefinanceinstitute.com/resources/cryptocurrency/simple-agreement-for-future-tokens-saft/.
[43] Andrey Sergeenkov, *What is a Crypto Airdrop*, *COINDESK* (May 11, 2023), https://www.coindesk.com/learn/what-is-a-crypto-airdrop/.
[44] *Id.*
[45] Mike Price, *What is a Retail Investor?*, THE MOTLEY FOOL (July 24, 2023), https://www.fool.com/terms/r/retail-investor/.
[46] *Products*, Coinbase, https://www.coinbase.com/products.

engage in traditional spot trading of cryptocurrencies, but they also offer subscriptions that include advanced trading tools such as technical analysis and advanced metrics.[47]

Institutions. Prominent CEXs have a long roster of products and services they offer only to non-profits, businesses, brokerages, and other institutions. Several exchanges will execute trades and reserve a buffet of over the counter (OTC) services—accompanied by deep aggregate liquidity, financing (lending, margin, and shorting), and personalized execution services—for institutional clients.[48] As they do for individual clients, the CEXs offer these clients access to a wide range of digital assets, but typically supported by individualized customer service.[49] The products and services are supported by the exchanges' integrated prime-brokerage and asset-management solutions, essentially enabling them to be one-stop shops for institutional clientele.[50] Additionally, CEXs offer custodial and staking services to institutional clients, and they provide these clients with comprehensive data not available to retail clients.

Developers. Developers and businesses seeking to build out cryptocurrencies and crypto products are a rapidly growing part of the CEX customer base. CEXs typically offer a comprehensive suite of tools to these clients, which might include Application Program Interfaces (APIs) for trading data or the opportunity to engage in the entire decentralized application (DApp) development process. CEXs offer APIs and software development kits (SDKs)—which allow developers to customize wallets or simply integrate a CEX wallet with an app—staking services, payment processing systems that use crypto, identity, and security services, and, of course, trading execution and data.[51] Some CEXs even have their own open-source tools to facilitate developers with blockchain integration.[52]

8. Types of Digital Assets

CEXs have many different types of digital assets available for trading on their platforms, including fungible tokens (including cryptocurrencies), non-fungible tokens, and derivatives.

Fungible Tokens. An asset is considered fungible when its units are interchangeable with one another. This means that the asset's units are indistinguishable and have the exact same validity and market value (e.g., bitcoin).

---

[47] *E.g.*, Coinbase Advanced, https://www.coinbase.com/advanced-trade; *Kraken Pro,* https://pro.kraken.com.

[48] *E.g.*, Coinbase Institutional, https://www.coinbase.com/institutional; Binance Institutional Services, https://www.binance.com/en/vip-institutionalservices; Kraken Account Management, https://www.kraken.com/features/account-management.

[49] *Id.*

[50] *See, e.g.*, Coinbase Prime, https://www.coinbase.com/prime.; Binance Asset Management, https://www.binance.com/en/assets-management.

[51] Coinbase Cloud, https://www.coinbase.com/cloud; Binance Cloud, https://cloud.binance.com.

[52] https://docs.cloud.coinbase.com/rosetta/docs/welcome.

- **Utility Tokens.** These are designed to give access to a specific platform, product, service, or functionality within a blockchain ecosystem. Utility tokens enable holders to interact with platforms by representing ownership or usage rights and can be used to pay for transactions or to access certain platform features.
- **Governance Tokens.** These allow platforms to engage with their asset-holders by conferring platform-related voting rights on them. Governance tokens often allow holders to propose and vote on changes, upgrades, or other matters related to the platform or network.
- **Stablecoins.** These assets are designed to maintain a stable market price, typically by pegging their value to the price of another asset.

Non-Fungible Tokens. NFTs are tokenized versions of digital or real-world assets that function as proofs of authenticity and ownership. Unlike fungible tokens, they are not interchangeable for others and rely on scarcity to drive value. Unique platforms and frameworks have been created to facilitate the issuance of NFTs.

Derivatives. In each instance (e.g., options, futures, etc.), the value of each product or contract is determined by an underlying asset. Digital asset derivatives may play a role in increasing liquidity of digital asset portfolios, mitigating their risks and diversifying them, which may also attract more investors, both individual and institutional. CEXs offer a varying number of derivative products to consumers depending on the jurisdiction. Some offer only derivative products, such as Ether and Bitcoin futures, while others offer a wide range of derivatives which vary in complexity.[53]

9. CEX Lines of Business

CEXs make money through fees from transactions, and via lending and other services, including staking and wallets.

Trading Commissions and Fees. CEXs generate a large portion of their revenue from the transaction fees they charge to customers for executing trades on their platform. These fees are typically a percentage of the transaction value.

Lending. CEXs also generate revenue by acting as intermediaries between lenders and borrowers. CEXs charge borrowers higher interest rates than the rates paid to lenders, creating a spread that generates profit.

Other Services. CEXs generate revenue by offering customers the opportunity to stake their cryptocurrencies on the platform, as well. They also charge fees for holding and safeguarding customer assets and earn interest on idle or unused cryptocurrencies held in custody.

---

[53] *E.g.*, Kraken Futures, https://www.kraken.com/features/futures; Coinbase Derivatives, https://www.coinbase.com/derivatives; Binance Options, https://www.binance.com/en/eoptions/ETHUSDT.

B. Overview of CEX Services

1. Simple v. advanced trading experiences

CEXs may offer different trading experiences depending on the sophistication of the user and fees the user is willing to pay. Simple trading typically entails the use of a basic CEX interface which includes services such as fixed price quotes and recurring trades. Some CEXs also offer a more advanced trading experience which includes, among other features, access to real-time market information, interactive charts, order books, and live trade history.

2. Pricing

CEXs may offer different pricing options for trading:

- **A la carte**. Transactions fees and a spread, which is added to the transaction. These fees are typically fixed as a percentage of volume.
- **Flat fees**. A percentage rate or fixed amount per transaction for small trading volume.
- **Subscription**. In lieu of a transaction fee, customers pay a monthly fee, until reaching a certain trading volume threshold.
- **Maker-taker**. This fee model incentivizes trades that remain on the order book and can be seen by other traders. The idea is that the open orders drive liquidity.

3. Wallets, Custodial Services, and Other CEX Product Offerings

Self-custody wallets v. custodial wallets. With a self-custody wallet, customers manage their private keys through a provider; custodial wallets are managed by CEXs. With a wallet on a centralized platform, users can safeguard their cryptocurrency with an intermediary and access their crypto balances directly on the exchange platform.[54] A user with a "self-custody" wallet must deal with a complex storage process involving unique, private keys that, if misplaced, could result in a total loss of crypto assets with no chance of recovery.[55] A CEX stores and secures a user's private keys and wallet, eliminating the risk of a user losing access. This can be highly beneficial for users, of

---

[54] *The State of Centralized Exchanges*, CRYPTOPEDIA, (April 6, 2021), https://www.gemini.com/cryptopedia/centralized-exchanges-crypto#section-services-offered-by-centralized-exchanges.

[55] Jake Frankenfeld, *Cold Storage: What It Is, How It Works, Theft Protection* (December 3, 2023), https://www.investopedia.com/terms/c/cold-storage.asp; Ryan Browne, Man makes last-ditch effort to recover $280 million in bitcoin he accidentally threw out, CNBC (January 15, 2021), https://www.cnbc.com/2021/01/15/uk-man-makes-last-ditch-effort-to-recover-lost-bitcoin-hard-drive.html.

course, though a CEX is still vulnerable to fraud, security breaches, and hacking, which could result in the loss of crypto holdings.[56]

Staking and Staking as a Service. Several CEXs offer users the opportunity to earn interest on their crypto through various staking and mining mechanisms, although the SEC has alleged that these services are a form of unregistered securities.[57] Customers deposit funds into the CEX platform, provide the CEX with access to their private keys, and pay a fee to the CEX; in exchange, the CEX handles the staking process.[58] Using CEX staking services can be advantageous for beginners and individuals who value deep liquidity and lower staking requirements, but customers may reap smaller staking rewards (due to the deduction of CEX staking fees), and be faced with penalties (if the CEX doesn't follow protocols) and cybersecurity breaches.[59]

Credit. Some CEXs also offer credit options to individuals, either through a credit card that rewards users with "crypto back" or through a direct loan secured by crypto assets.[60] Customers can set up direct deposits through CEXs as well; they can typically elect the assets to be deposited as fiat or automatically converted to the supported cryptocurrency of their choice.[61]

C. CEX Business Risk Factors

Cybersecurity. Cyberattacks and security breaches of CEX platforms—or those impacting CEX customers through third parties—could obviously adversely impact CEX reputation and business, results, and financial condition.

Centralized exchanges rely on their own closed systems, which, like any other online business that custodies assets and holds other personal information, will have some vulnerability to hacking and fraud—no matter the strength of the security protections in place.

Examples

Mt. Gox: In 2014, Mt. Gox, once the world's largest Bitcoin exchange, suffered a massive hack that resulted in the theft of approximately 850,000 Bitcoins, valued at over $450 million. The breach exposed vulnerabilities in Mt. Gox's security and

---

[56] The Federal Trade Commission, *What to Know About* Cryptocurrency *and Scams,* https://consumer.ftc.gov/articles/what-know-about-cryptocurrency-and-scams.

[57] *E.g.* Coinbase Earn, https://www.coinbase.com/earn; Binance Earn, https://www.binance.com/en/earn.

[58] *Decentralized Staking vs. Centralized Staking*, TRUST WALLET (March 27, 2023), https://blog.trustwallet.com/blog/decentralized-staking-vs-centralized-staking.

[59] *Id.*

[60] *E.g.*, Coinbase Card, https://www.coinbase.com/card; Binance Cards, https://www.binance.com/en/cards.

[61] Coinbase Direct Deposit, https://www.coinbase.com/direct-deposit.

management practices, ultimately leading to its bankruptcy and subsequent legal proceedings.[62]

Coincheck: In 2018, hackers exploited a vulnerability in Coincheck's systems, stealing approximately 500 million NEM tokens, valued at $523 million. The breach prompted regulatory scrutiny and Coincheck reimbursed affected users.[63]

KuCoin: In 2020, hackers exploited vulnerabilities in KuCoin's hot wallets and stole an estimated $280 million in various cryptocurrencies.[64] KuCoin responded by identifying affected assets, cooperating with other exchanges to freeze and recover stolen funders, and enhancing its security measures.[65]

Private Keys. If a user loses the private keys to a self-custody wallet, they lose the ability to access or transfer the crypto in that wallet. Users opt into CEX custodial services in part because they trust the institution to keep their private keys secure. But as any security breach shows, a risk of theft, loss, or destruction of private keys still exists. If a CEX is unable to access its private keys or is hacked, the CEX could also lose access to its crypto. Needless to say this would also result in increased regulatory scrutiny, reputational harm, and other damage.

VPN circumvention. For a variety of reasons, including regulatory compliance, CEXs restrict users from various jurisdictions. This does not keep some users from attempting to conceal their location by using a Virtual Private Network to show an IP address to the CEX that is different from their actual IP address. This practice causes concern about security risks, legality, compliance issues, and would raise red flags with regulators, too.

"Run on the Exchange." Unlike traditional stock exchanges, which regulations require to have daily trading limits, CEXs are typically open 24/7. Large crypto investors are not prohibited from making substantial withdrawals or transfers over a short period. Likewise, external market forces, including noise from social media, can trigger or accelerate a run on a particular CEX, and investors would not be restricted from withdrawing or transferring assets, which could lead to additional volatility in the crypto market. This is primarily a risk for CEXs that offer high leverage and margin trading options, which expose traders to significant risks and where customer assets are

---

[62] Carter Dougherty & Grace Huang, *Mt. Gox Seeks Bankruptcy After $480 Million Bitcoin Loss*, BLOOMBERG (February 28, 2014), https://www.bloomberg.com/news/articles/2014-02-28/mt-gox-exchange-files-for-bankruptcy.

[63] Sarah Ahmed, *Coincheck Hack – One of the Biggest Crypto Hacks in History*, COINMARKETCAP (2021), https://coinmarketcap.com/alexandria/article/coincheck-hack-one-of-the-biggest-crypto-hacks-in-history; Wolfie Zhao, *Regulators Probe Coincheck's Hack Compensation Claims*, COINDESK (February 2, 2018), https://www.coindesk.com/markets/2018/02/02/regulators-probe-coinchecks-hack-compensation-claims/.

[64] Aha Hui & Wolfie Zhao, *Over $280M Drained in KuCoin Crypto Exchange Hack*, COINDESK (September 26, 2020), https://www.coindesk.com/markets/2020/09/26/over-280m-drained-in-kucoin-crypto-exchange-hack/.

[65] *Id.*

not backed 1:1.[66] If market conditions change rapidly, a significant number of traders may try to exit their positions simultaneously, leading to potential liquidity issues for the CEX.[67]

Trading Market Share by Certain Assets. CEX revenue from trades tends to be highly concentrated in Bitcoin and Ethereum transactions.[68] If revenue from these transactions declines and is not replaced by new demand for other digital assets or other services, the CEX's business, operating results, and financial condition could be adversely affected.

1. Stage of Development and Volatility.

Nascent technology. Digital assets and CEXs are relatively new. Many products and exchanges are unlicensed and unregulated, and do not provide the public with information about ownership structure, corporate practices, or regulatory compliance. As a result, customers and the general public may lose confidence or interest in digital assets and digital asset platforms, including CEXs.

Price cycles and volatility. Operating results have historically fluctuated, and they will likely continue to fluctuate significantly, in part due to the highly volatile nature of digital assets. A CEX's total revenue depends on the prices of crypto assets and the volume of transactions on its platform. If price or volume declines, the CEX's business, operating results, and financial condition would be adversely affected.

2. Regulatory Landscape.

Domestic. CEXs are entangled in an extensive, evolving, and uncertain regulatory landscape in the U.S. Any adverse change to or failure to comply with laws and regulations can harm an exchange's business. Not only are there regulations for the operation of the CEXs themselves, but there are also regulations governing their operation as clients of other banking institutions and *their* clients. Specific regulatory issues are addressed in Section D.

International. CEXs operate in a highly competitive industry and compete against unregulated, or at least less regulated, foreign companies, and a CEX's business,

---

[66] Ekin Genç, *What is Margin Trading? A Risky Crypto Trading Strategy Explained,* COINDESK (November 15, 2022), https://www.coindesk.com/learn/what-is-margin-trading-a-risky-crypto-trading-strategy-explained/; Paige Tortorelli, Sam Bankman-Fried's Alameda quietly used FTX customer funds for trading, say sources, (November 13, 2022), https://www.cnbc.com/2022/11/13/sam-bankman-frieds-alameda-quietly-used-ftx-customer-funds-without-raising-alarm-bells-say-sources.html; Alesia Haas, *Our approach to transparency, risk management, and consumer protection,* (November 8, 2022), https://www.coinbase.com/blog/our-approach-to-transparency-risk-management-and-consumer-protection.

[67] *See* Genç, *supra* note 66. *See* Totorelli, *supra* note 66.

[68] Bitcoin Price, COINMARKETCAP, https://coinmarketcap.com/currencies/bitcoin/; Ethereum Price, COINMARKETCAP, https://coinmarketcap.com/currencies/ethereum/.

operating results, and financial condition may be adversely affected if domestic regulations render it unable to respond to its competitors effectively.

D. Legal Issues for CEXs

Many CEXs operate in an uncertain and evolving legal and regulatory landscape. As courts and regulators understand more about CEXs and the assets that are traded on their platforms, CEXs must be prepared to consider modifying their businesses in response to legal and regulatory developments.

1. Alleged Securities and Exchange Commission Violations

The SEC has already undertaken significant enforcement actions in the cryptocurrency sphere. The SEC has moved in the direction of regulating digital assets as traditional securities and platforms as entities that perform unregistered exchange actions, broker-dealer activities or clearing—whether as an exchange, a broker-dealer, or a clearing agency. In an April 4, 2022 speech, SEC Chairman Gary Gensler stated that cryptocurrency trading and lending platforms, both centralized and otherwise, "likely are trading securities."[69] He also noted that one of the SEC's "projects" was to register cryptocurrency platforms "much like exchanges."[70] Chairman Gensler reiterated this position on March 9, 2023, stating that centralized exchanges are likely exchanges as defined by the Exchange Act and therefore must register.[71] In this section, we address the types of relief available against exchanges and then elaborate on theories of liability.

a. Types of enforcement actions available against an exchange

Cease and desist proceedings initiated by the SEC under Section 21C of the Exchange Act. Depending on the circumstances, an order that a CEX cease and desist from engaging in what the SEC deems violating securities laws would make it difficult, if not impossible, for a digital asset exchange to continue operating. Often, cease and desist proceedings result in a consent order in which the CEX submits an offer of settlement. To take one example, in the SEC's enforcement actions against Kraken in February 2023, Kraken did not admit or deny the findings in order, but simply

---

[69] Gary Gensler, Chair of the Securities and Exchange Commission, Prepared Remarks of Gary Gensler On Crypto Markets, Penn Law Capital Markets Association Annual Conference, (April 4, 2022), https://www.sec.gov/news/speech/gensler-remarks-crypto-markets-040422.

[70] *Id.*

[71] Gary Gensler, *Getting crypto firms to do their work within the bounds of the law*, THE HILL, (March 9, 2023), https://thehill.com/opinion/congress-blog/3891970-getting-crypto-firms-to-do-their-work-within-the-bounds-of-the-law/.

consented to entry of the order, which required the CEX to discontinue selling crypto asset–staking services and products.

Civil suits brought by the SEC under Section 20 of the Exchange Act. Much like a cease-and-desist order, a civil suit would likely make it very difficult for an exchange to continue operating. These actions too are often settled.

b. Types of relief available against an exchange

The SEC may seek a variety of relief under Section 20(d) of the Securities Act, 15 U.S.C. § 77t, or Section 21(d)(3) of the Exchange Act, 15 U.S.C. § 78u. As noted above, the administrative proceedings and civil suits instituted against exchanges often settle, with the exchange agreeing to one or more of the following:

- Monetary relief, such as disgorgement, civil penalties, and prejudgment interest;
- Injunctive relief (if in federal court),[72] often enjoining the exchange from violating the Securities and Exchange Acts; and/or
- An independent monitor.

c. Types of Violations Alleged

Operating as an unregistered securities exchange under Section 5 of the Exchange Act. One of the primary risks for centralized exchanges is operating without registering with the SEC. Here are some examples:

- **In re Poloniex**: Poloniex agreed to the SEC's entry of a cease-and-desist order, which included the claim that Poloniex had failed to register as a securities exchange under Section 5 of the Exchange Act when it operated as a digital asset trading platform.[73] Although Poloniex sold its trading platform in 2019, two years before the cease-and-desist proceedings, the SEC found that it had operated as an unregistered exchange before then. The order specifically noted that Poloniex had allowed trading of digital assets that the platform internally characterized as "medium risk" of being securities.
- **SEC v. BitFunder**: BitFunder agreed to the SEC's entry of a cease-and-desist order, which provided that BitFunder had failed to register as a securities exchange under Section 5 of the Exchange Act.[74] In addition, the CEO of

[72] *See* 15 U.S.C. § 77t(b) (stating that injunctive relief may be sought "in any district court of the United States, or United States court of any Territory…"); 15 U.S.C. § 78u(d)(1) (same).
[73] *In re Poloniex*, ORDER INSTITUTING CEASE-ANDDESIST PROCEEDINGS PURSUANT TO SECTION 21C OF THE SECURITIES EXCHANGE ACT OF 1934, MAKING FINDINGS, AND IMPOSING A CEASEAND-DESIST ORDER, File No. 3-20455, (2021), https://www.sec.gov/files/litigation/admin/2021/34-92607.pdf.
[74] Complaint, *SEC v. Jon E. Montroll and Bitfunder*, No. 1:18-cv-01582, (S.D.N.Y, 2018), https://www.sec.gov/files/litigation/complaints/2018/comp-pr2018-23.pdf.

BitFunder was sentenced to 14 months in prison for lying to the SEC and defrauding customers.[75]

Operating as an unregistered broker-dealer in violation of Exchange Act Section 15(a). Section 15(a) of the Exchange Act requires broker-dealers to register.[76] If a digital asset exchange is found to have "effect[ed] any transactions in, or to [have] induc[ed] or attempt[ed] to induce the purchase or sale of, any security" without registering as a broker-dealer, it may be in violation of Section 15(a).

- **In re BTC Trading Corp**: BTC Trading Corp agreed to the SEC's entry of a cease-and-desist order finding that BTC Trading operated two online exchanges that failed to register as broker-dealers in violation of § 15(a) and failed to register as exchanges in violation of Section 5 of the Exchange Act.[77]
- **SEC v. Beaxy**: The SEC sued Beaxy.com, Windy Inc. (the entity created to operate Beaxy.com), and former executives of the companies, among others, in the Northern District of Illinois for Section 15(a) and Section 5 violations.[78] Windy was alleged to have facilitated crypto asset transactions, charged a fee, and solicited and recruited investors. Although Beaxy and Windy were not exchanges, they were alleged to have stated that the proceeds from the ICO of BXY—the Beaxy token—would be used to develop a "crypto asset trading platform." The current executives of Beaxy.com agreed to shut down the platform in exchange for a dismissal of the charges.[79]

Operating as an unregistered clearing agency in violation of Exchange Act Section 17A. Section 17A of the Exchange Act requires clearing agencies to register with the SEC. An entity is considered a clearing agency if it "interposes itself between the counterparties to securities transactions, acting functionally as the buyer to every seller

---

[75] Stewart Bishop, *Bitcoin Co. Boss Gets 14 Months For Lying To SEC*, LAW360, (July 11, 2019), https://www.law360.com/articles/1177572/bitcoin-co-boss-gets-14-months-for-lying-to-sec.
[76] *See* 15 U.S.C. § 78o(a).
[77] *In re BTC Trading, Corp. and Ethan Burnside*, ORDER INSTITUTING ADMINISTRATIVE AND CEASE-AND-DESIST PROCEEDINGS PURSUANT TO SECTION 8A OF THE SECURITIES ACT OF 1933, SECTIONS 15(b) AND 21C OF THE SECURITIES EXCHANGE ACT OF 1934, AND SECTION 9(b) OF THE INVESTMENT COMPANY ACT OF 1940, MAKING FINDINGS, AND IMPOSING REMEDIAL SANCTIONS AND A CEASEAND-DESIST ORDER, File No. 3-16307, (2014), https://www.sec.gov/files/litigation/admin/2014/33-9685.pdf#:~:text=This%20matter%20involves%20two%20enterprises%20--%20LTC-Global%20Virtual,LTC-Mining%2C%20another%20virtual%20currency%20enterprise%20founded%20by%20Burnside.
[78] Complaint, *SEC v. BEAXY DIGITAL, LTD., ARTAK HAMAZASPYAN, WINDY INC., NICHOLAS MURPHY, RANDOLPH BAY ABBOTT, BRAVEROCK INVESTMENTS, LLC, FUTURE DIGITAL MARKETS, INC., WINDY FINANCIAL LLC, FUTURE FINANCIAL LLC, AND BRIAN PETERSON*, No. 1:23-cv-01962, (N.D.I.L., 2023), https://www.sec.gov/files/litigation/complaints/2023/comp-pr2023-64.pdf.
[79] Jessica Corso, *Crypto Platform Beaxy Shuttered as SEC Pursues Founder*, *LAW360* (March 29, 2023), https://www.law360.com/articles/1591349/crypto-platform-beaxy-shuttered-as-sec-pursues-founder.

and the seller to every buyer."[80] The SEC has alleged that some digital asset exchanges are unregistered clearing agencies.

- SEC v. Beaxy: As described above, the SEC sued several entities, including Windy Inc., which was alleged to have violated § 17A because it held customers' securities as "custodial assets" in "Windy-controlled wallets" and subsequently settled the smart-contract transactions. As noted, the charges were dismissed against Windy and Beaxy.[81]

Selling unregistered securities & investment contracts. Section 5(a) of the Securities Act prohibits the sale of unregistered securities and investment contracts. Any CEX liability here depends on the status of the assets the CEX offers—if the assets listed are considered "securities," the CEX may be at risk.

- SEC v. Ripple: The recent Southern District of New York decision in *SEC v. Ripple* offers some reassurance to CEXs that list assets alleged to be securities by the SEC.[82] The court granted partial summary judgment to Ripple, concluding that Ripple's sales of its token, XRP, to the general public on exchanges did not constitute unregistered security sales. After the court denied the SEC's request for an interlocutory appeal, the SEC voluntarily dismissed the charges against the individual Ripple defendants, and the case remains ongoing.

- SEC v. Bitqyck: The SEC filed a suit against Bitqyck Inc. and its founders in the Northern District of Texas, alleging that Bitqyck failed to register as an exchange when it created its own trading platform—TradeBQ.com.[83] The SEC also alleged that Bitqyck created and sold unregistered securities on the TradeBQ exchange, in violation of Section 5(a). Bitqyck consented to a final judgment that included injunctive relief and payment of disgorgement, prejudgment interest, and a civil penalty of $8,375,617. The two founders of Bitqyck also consented to entry of a final judgment of injunctive relief, payment of disgorgement, prejudgment interest, and a civil penalty of $890,254 and $850,022, respectively. [84]

- SEC v. Payward: The SEC filed suit against Payward d/b/a Kraken, alleging that Kraken's staking program was, in fact, an investment contract and therefore

---

[80] *Clearing Agencies,* U.S. Securities and Exchange Commission, https://www.sec.gov/tm/clearing-agencies#:~:text=Clearing%20Agencies.%20Section%2017A%20of%20the%20Securities%20Exchange,meet%20the%20standards%20set%20forth%20in%20Section%2017A.

[81] *See SEC v. Beaxy*, *supra* note 78.

[82] Complaint, *SEC v. RIPPLE LABS, INC., BRADLEY GARLINGHOUSE, and CHRISTIAN A. LARSEN*, No. 1:20-cv-10832-AT-SN (S.D.N.Y, 2023), https://www.nysd.uscourts.gov/sites/default/files/2023-07/SEC%20vs%20Ripple%207-13-23.pdf.

[83] Complaint, *SEC v. BITQYCK, INC., BRUCE E. BISE, and SAMUEL J. MENDEZ,* No 3:19-cv-02059-N (N.D. TX, 2019), https://www.sec.gov/files/litigation/complaints/2019/comp-pr2019-164.pdf.

[84] SEC Charges Dallas Company and Its Founders with Defrauding Over 13,000 Investors in Unregistered Offering and Operating Unregistered Digital Asset Exchange, No. 3:19-cv-2059-N, Release No. 24582 (N.D. TX, 2019), https://www.sec.gov/litigation/litreleases/lr-24582.

should have been registered.[85] Kraken and the SEC settled, with Kraken agreeing to cease offering or selling securities through the staking program and to pay $30 million in disgorgement, prejudgment interest, and civil penalties.[86]

Selling unregistered security-based swaps. Section 5(e) of the Securities Act prohibits the sale of security-based swaps without registration if the buyer is not an eligible contract participant—*i.e.*, a corporation, a broker, or a high net-worth individual. *See* 7 U.S.C. § 1a(18). Section 6(I) further provides that security-based swaps must occur on national exchanges.

- In re Sand Hill Exchange: Sand Hill agreed to the SEC's entry of a cease-and-desist finding that had Sand Hill violated Sections 5(e) and 6(I) of the Securities Act.[87] The SEC accused Sand Hill of selling contracts linked to specific companies, their securities values, and other liquidity events. Sand Hill was a centralized exchange, built on the Bitcoin blockchain, which allowed users to deposit dollars or bitcoin for their orders.

d. Individual Liability

Individuals associated with exchanges that are alleged to have failed to register may also face liability.

Control person liability. Individuals may face liability if the entity they controlled was an unregistered exchange under Section 20(a) of the Exchange Act. Liability under Section 20(a) requires the SEC to allege a primary violation, control of the primary violator by the defendant, and that the defendant was a culpable participant.

- In re EtherDelta: EtherDelta and its creator, Zachary Coburn, agreed to the SEC's entry of a cease-and-desist order against him.[88] The order found that EtherDelta had operated as an exchange in violation of Section 5 and that Coburn should have known that his actions, in creating and running EtherDelta, would contribute to EtherDelta's violations.

---

[85] Complaint, *SEC v. Payward Ventures, Inc. and Payward Trading, LTD*, No. 23-cv-588, (N.D. CA 2023), https://www.sec.gov/files/litigation/complaints/2023/comp-pr2023-25.pdf.

[86] Press Release, Kraken to Discontinue Unregistered Offer and Sale of Crypto Asset Staking-As-A-Service Program and Pay $30 Million to Settle SEC Charges, (2023), https://www.sec.gov/news/press-release/2023-25.

[87] In re *Sand Hill Exchange, Gerrit Hall and Elaine Ou*, ORDER INSTITUTING CEASE-ANDDESIST PROCEEDINGS PURSUANT TO SECTION 8A OF THE SECURITIES ACT OF 1933 AND SECTION 21C OF THE SECURITIES EXCHANGE ACT OF 1934, MAKING FINDINGS, AND IMPOSING A CEASE-AND-DESIST ORDER, File No. 3-16598, (2015), https://www.sec.gov/files/litigation/admin/2015/33-9809.pdf.

[88] *In re Zachary Coburn*, ORDER INSTITUTING CEASE-ANDDESIST PROCEEDINGS PURSUANT TO SECTION 21C OF THE SECURITIES EXCHANGE ACT OF 1934, MAKING FINDINGS, AND IMPOSING A CEASEAND-DESIST ORDER, File No. 3-18888, (2018), https://www.sec.gov/files/litigation/admin/2018/34-84553.pdf.

- SEC v. BitFunder: The SEC alleged that the CEO of BitFunder was a control person of BitFunder's Section 5 violation since he was BitFunder's operator and creator.[89] As noted, the civil suit settled after the CEO was sentenced to 14 months in prison for lying to the SEC and defrauding customers.[90]

Aiding and abetting liability. An individual could be charged with aiding and abetting an exchange's failure to register under Section 20(e) of the Exchange Act or Section 15(b) of the Securities Act. In theory, an exchange could also potentially be liable under Section 20(e) for "aiding and abetting" a primary violator of SEC regulations. The exchange would need to have scienter with regard to the violation and provide substantial assistance to be considered in violation. Because secondary theories of liability have not been asserted against CEXs for the violations of digital asset issuers, the level of "substantial assistance" necessary to be considered an aider and abettor is unclear. For example, it is unclear if listing an unregistered digital asset that is found to be a security would be considered "substantial assistance," but any ruling may depend on what the exchange knew or had reason to know about the risk of the asset being deemed a security.

- SEC v. Bitqyck: Bitqyck Inc. was alleged to have failed to register as an exchange when it created its own trading platform, TradeBQ.com.[91] The two creators of Bitqyck were charged with aiding and abetting Bitqyck's failure to register. As noted, the founders consented to entry of a final judgment of injunctive relief, payment of disgorgement, prejudgment interest, and a civil penalty of $890,254 and $850,022, respectively.[92]

2. Commodity Futures Trading Commission Regulations (Commodity Exchange Act)

In addition to selling "traditional" crypto tokens, platforms now trade in crypto derivatives—tokens that derive their value from something else. That something else can be the performance of another crypto token or fiat currency, or even the occurrence (or nonoccurrence) of an event in the real world. This includes crypto options. For example, if you purchase an Ether call option for $1,000 with a strike price of $10,000 and an expiration date of ten weeks, you would pay $1,000 upfront and have the right to purchase Ether in ten weeks for $10,000—no matter what the price of Ether is on that day.

Depending on the type of asset that is traded on a CEX, the exchange may qualify as a Future Commission Merchant, which is defined as an entity that solicits or accepts orders for transactions involving futures, swaps, commodity options, or retail

[89] *See SEC v. Jon E. Montroll and Bitfunder*, supra note 74.
[90] *See* Bishop, *supra* note 75.
[91] *See SEC v. BITQYCK, INC., BRUCE E. BISE, and SAMUEL J. MENDEZ*, supra note 83.
[92] *Supra* note 84.

commodity transactions, or which accepts money to margin, guarantee or secure trades contracts.

Similarly, an exchange may also qualify as a Designated Contract Market or Swap Execution Facility (SEF) if it allows trading of swaps of digital asset commodities, which the CFTC has said include Bitcoin, Ether, Litecoin, and other tokens. An SEF matches buyers and sellers of swap contracts, which is similar to options and futures contracts except they have no expiration dates. Both designations require registration with the CFTC.

Not many crypto platforms are registered with the CFTC, but the agency has previously approved applications for licenses to offer crypto-derivatives products. For example, in 2016, the CFTC granted Clear Markets North America, a platform that offers crypto-derivative trading for U.S. dollar–Bitcoin, to operate as an SEF to trade in and offer swaps.

3. Customer Registration Requirements

Since CEXs provide digital-asset access to a broad range of customers, and because the U.S. is especially wary of criminals using such assets to circumvent traditional security measures for foreign transfers and money laundering, CEXs in the U.S. generally must comply with the Know Your Customer (KYC) and Anti-Money Laundering (AML) regimes to operate their businesses.[93]

KYC procedures allow CEXs to verify the identity of their users, typically by requiring customers to submit their personal information and government identification.[94] CEXs use this personal information to assign risk values to customers based on their likelihood of committing financial crimes.[95] This information also helps the CEXs prevent fraud by allowing them to verify their customers' identification.

AML rules are in place to prevent criminals from using CEXs to launder money—they would convert illegally obtained cryptocurrencies into fiat currencies and then withdraw the funds.[96]

In the U.S., the Financial Crimes Enforcement Network (FinCEN) requires every exchange that deals with cryptocurrency to implement KYC and AML programs, in addition to Combating the Financing of Terrorism regime.[97] The most recent FinCEN guidance requires Money Service Businesses—which include CEXs—"to develop,

---

[93] *What is KYC, and Why do Crypto Exchanges Require It?*, COINDESK, https://cointelegraph.com/learn/what-is-kyc-and-why-do-crypto-exchanges-require-it.
[94] *Id.*
[95] *The 2023 Guide to KYC/AML for Crypto Exchanges & Wallets*, CHECK IN (January 17, 2022), https://getId.com/aml-kyc-crypto-exchanges-wallets/.
[96] *What is AML/KYC in Crypto?*, DEFI PLANET (April 19, 2022), https://defi-planet.com/2022/04/what-is-aml-kyc-in-crypto/.
[97] *Id.*

implement, and maintain an effective written anti-money laundering program." It can be found in FinCEN's 2019 Guidance on Convertible Virtual Currencies.[98]

4. Private Actions

In addition to regulatory enforcement actions, private plaintiffs have also sued CEXs, not only for violations of state and federal securities and commodities laws, but also for alleged violations of state consumer protection laws.

For example, in April 2020, one New York–based law firm filed 11 class action lawsuits against various exchanges,[99] including:

- **Binance**: The complaint alleged that Binance failed to register as an exchange and subsequently made unregistered offers and sales of securities under Section 5 of the Exchange Act and failed to register as a broker-dealer under Section 15(a)(1) of the Exchange Act. Plaintiffs utilized Section 29(b) of the Exchange Act, which allows plaintiffs to void contracts they entered which violated the Exchange Act, including under Section 5.[100] They further alleged that Binance violated the Texas Securities Act, Tex. Rev. Civ. Stat. art. 581-33, which prohibits unregistered security sales. The complaint also alleged control-person liability against Binance's executives.
- **BitMEX**: Similar allegations were made against HDR Global Trading Limited, the owner and operator of cryptocurrency platform BitMEX.[101] In addition to Exchange Act violations for failing to register (1) as an exchange, (2) as a broker-dealer, and (3) the token sales themselves, the plaintiffs alleged market manipulation in violation of Section Section 6 and 22 of the Commodities Exchange Act. Plaintiffs also alleged various violations of secondary liability, including control-person liability, aiding and abetting, and principal-agent liability under the Commodities Exchange Act. In addition to allegations under Texas law similar to those in the Binance case, the plaintiffs here alleged violations of the New Jersey Uniform Securities Law for failing to register BitMEX's token sales.

---

[98] *Application of FinCEN's Regulations to Certain Business Models Involving Convertible Virtual Currencies*, FIN-2019-G001 (May 9, 2019), https://www.fincen.gov/sites/default/files/2019-05/FinCEN%20Guidance%20CVC%20FINAL%20508.pdf.

[99] Amy Castor and Tim Copeland, *Class-action Lawsuits Filed Against 11 Crypto Companies*, (April 4, 2020), https://decrypt.co/24532/class-action-lawsuits-filed-against-7-bitcoin-companies.

[100] Complaint, *ERIC LEE and CHASE WILLIAMS v. BINANCE, CHANGPENG ZHAO, YI HE, and ROGER WANG*, 1:20-cv-02803, (S.D.N.Y. 2020), https://wp.decrypt.co/wp-content/uploads/2020/04/binance-120-cv-02803.pdf.

[101] Complaint, *CHASE WILLIAMS and WILLIAM ZHANG v. HDR GLOBAL TRADING LIMITED, ABS GLOBAL TRADING LIMITED, ARTHUR HAYES, BEN DELO, and SAMUEL REED*, 1:20-cv-02805 (S.D.N.Y. 2020), https://wp.decrypt.co/wp-content/uploads/2020/04/Zhang_et_al_v_HDR_Global_Trading_Limited_et__nysdce-20-02805__0001.0-1.pdf.

A 2023 study by Bloomberg Law found that suits dealing with cryptocurrency hacking have, not surprisingly, risen dramatically in recent years, and 13 of those actions were brought against CEXs or entities offering custodial services.[102] As noted, this is a risk factor for the business of CEXs, and these civil suits indicate that CEXs should consider the potential for litigation in the event of a hack.

5. Money Transmission Licenses

Federal and state law requires money transmitters—those who transfer currency or value that substitutes for currency—to comply with a variety of requirements, including that they become licensed as a money transmitter and implement Anti-Money Laundering and Know-Your-Customer policies to detect and report suspicious transactions. At the federal level, the Bank Secrecy Act requires money transmitters to, among other things, implement an AML/KYC policy, designate an AML officer, and file Suspicious Activity Reports for transactions involving potential money laundering or terrorist finances.

CEXs are money transmitters under federal law. In 2013, FinCEN issued guidance affirmatively stating that a platform that either accepts and transmits a convertible virtual currency or that buys or sells convertible virtual currency "for any reason" is a money transmitter.

Separate and apart from federal money transmission obligations, states have regulatory and license requirements for CEXs as money transmitters. Some states have developed comprehensive requirements for crypto businesses and unique licenses, such as the New York BitLicense for companies engaged in "virtual currency business activities." This expressly includes receiving virtual currency for transmission or transmitting virtual currency, as well as storing, holding, or maintaining custody of virtual currency on others' behalf.

6. Office of Foreign Assets Control (OFAC) Economic Sanctions Compliance

All CEXs doing business in the U.S. are required to comply with sanctions rules issued by the Treasury Department's Office of Foreign Assets Control (OFAC). OFAC has issued crypto-specific guidance, including definitions for "digital currency" and "virtual currency," to clarify the scope and nature of a cryptocurrency business's obligations.

While many countries have economic sanctions laws, U.S. economic sanctions laws generally are the broadest and most aggressively enforced. A company's activities are

[102] Skye Witley, *Crypto Hack Lawsuits Rise as Theft Victims Try Untested Claims*, BLOOMBERG (January 3. 2023), https://news.bloomberglaw.com/privacy-and-data-security/crypto-hack-lawsuits-rise-as-theft-victims-try-untested-claims.

subject to the jurisdiction of U.S. economic sanctions laws if they are undertaken in the United States or involve "U.S. Persons." "U.S. Persons" include any U.S. citizen or U.S. permanent resident with oversight or support roles throughout a company's global operations; any entity organized under the laws of the United States (including non-U.S. branches of such companies); and any person or company acting in the territory of the United States (even if that person is a citizen of another country). U.S. economic sanctions consist of, among other things: (i) embargoes prohibiting virtually all business transactions between U.S. Persons and Cuba, Iran, North Korea, Syria, and regions of Ukraine occupied by Russia (Crimea, Donetsk, and Luhansk); and (ii) restrictions or prohibitions on business by U.S. persons with Specially Designated Nationals and Blocked Persons, wherever they may be located.

Failure to heed the restrictions imposed by OFAC's rules can have significantly adverse consequences. For companies subject to U.S. jurisdiction, violations of these rules can result in significant penalties. Exchanges that are not U.S. persons that facilitate activity with sanctioned parties can themselves be the target of economic sanctions. For example, in September 2021, OFAC designated a virtual currency exchange—SUEX OTC, S.R.O.—for facilitating financial transactions for at least eight ransomware actors. According to OFAC, over 40% of SUEX's known transactions were associated with illicit actors.

And in August 2022, OFAC sanctioned virtual currency mixer Tornado Cash for, among other things, allowing a North Korea–sponsored hacking group to launder more than $455 million worth of crypto.

The consequences of being sanctioned are significant. The property and interests in the U.S. or in the possession or control of a U.S. person are blocked and required to be reported to OFAC. Effectively, it results in losing the ability to conduct business with any U.S. person. Other countries may apply similar economic sanctions, which may restrict a company from doing business with certain countries or individuals.

Custodial Services

Lilya Tessler and Daniel Stabile*

A. Introduction

Custody is an important facet of digital asset[1] ownership, particularly because many digital assts have "bearer instrument" qualities. Generally, "digital asset custody" is a broad term that encompasses various methods of storing and safeguarding digital assets. A diverse and expanding range of custody solutions are available.

In contrast to traditional finance, blockchain technology is ideologically premised on the idea of disintermediation.[2] Rather than relying on financial institutions as trusted third parties to validate and facilitate transactions, blockchain users rely on cryptographically secure, shared software systems. Self-custody, in which the owner of a digital asset manages and secures their digital assets directly without reliance on a third party, is squarely rooted in this ideal. Nonetheless, as the market for digital assets has grown and evolved, the availability of third-party custodial services has rapidly emerged.

In the digital asset ecosystem, digital asset custodians ("DACs") may serve a similar role to traditional custodians, but they operate in different technological, operational, and legal environment. A DAC's essential role is to protect digital assets, primarily by safeguarding its customers' "private keys." As described below in Section B, keys,

---

* Tessler is a Partner at Sidley Austin LLP, in Dallas, TX (https://www.sidley.com/en/people/t/tessler-lilya-t); Stabile is a Partner at Winston & Strawn, LLP, in Miami, FL (https://www.winston.com/en/professionals/stabile-daniel-t). The authors appreciate the contributions of Kimberly Prior, Dhruva Krishna, Collin Groebe, and Gabriela Plasencia at Winston & Strawn LLP and of Daniel Engoren at Sidley Austin LLP. Sections A, C and E were drafted by lawyers at Winston & Strawn, and Sections B and D were drafted by lawyers at Sidley Austin. Michelle Gitlitz, General Counsel at Flexa Inc., reviewed this chapter.

[1] Usage and terminology in the marketplace vary. As used here, "digital assets" is a broad term referring to tokens that are created and/or transferred utilizing blockchain technology. There is a limitless number of different digital assets, each with their own properties and characteristics, which can result in various regulatory classifications. Depending on the circumstances, digital assets (or types of digital assets) may also be referred to as crypto assets, virtual currencies, coins, tokens, security tokens, cryptocurrencies, and a variety of other terms.

[2] *See* Satoshi Nakamoto, Bitcoin: A Peer-to-Peer Electronic Cash System (Oct. 31, 2008), available at: https://bitcoin.org/bitcoin.pdf.

including the corresponding "public key" and "private key," are tied to a "wallet." Wallets are described as "hot" or "cold," depending on the technology utilized, and store customers' private keys, while also facilitating transactions.

There are a variety of different custody options available to owners of digital assets. As described in Section C, these options range from self-custody of one's own assets, to the use of different types of service providers that act as third-party custodians.

Section D focuses on operational and contractual issues that should be considered when entering various custodial relationships. Finally, Section E discusses the primary regulatory issues relevant to digital asset custody arrangements.

B. Wallets and Keys: The Core of Digital Asset Custody

The essence of digital asset custody is to protect and maintain the ownership of digital assets by safeguarding a private key, typically through the use of digital wallets. Digital wallets describe software that enables a person to control and transfer digital assets to others. As discussed in further detail below, digital wallets allow users to generate and control a public and private key pair used to interact with a particular blockchain and to authorize a digital asset transaction. In other words, digital wallets provide a mechanism for customers to interact with a blockchain network and control digital assets. To understand digital asset custody, a user must have a foundational understanding of blockchain technology and digital assets.

1. Blockchain Technology

Blockchains are a type of distributed ledger technology. As ledgers, blockchains are fundamentally used for storing and managing data.[3] Blockchain technology uses asymmetric-key cryptography (also referred to as public key cryptography) to verify the integrity and authenticity of transactions. To settle a digital asset transaction, the transaction must be broadcast to the relevant blockchain network and confirmed by other users (nodes) on the network. Every blockchain is governed by its own technological rules, or protocols. While the descriptions in this chapter are generally applicable, a particular blockchain may have minor or substantial differences. This is especially true of private blockchains, which may have fundamentally different controls and processes that are not described here.

[3] *See* Nat'l Inst. of Standards & Tech., U.S. Dep't of Comm., NISTIR 8202, Blockchain Technology Overview (Oct. 2018). Available at https://nvlpubs.nist.gov/nistpubs/ir/2018/NIST.IR.8202.pdf.

2. Keys – Public and Private

In asymmetric-key cryptography, there are two corresponding types of keys – public and private. Public and private keys are used for a variety of functions on blockchain networks:

1. Private keys are used to digitally sign transactions.
2. Public keys are used to derive addresses.
3. Public keys are used to verify signatures generated with private keys.

Asymmetric-key cryptography provides the ability to verify that the user transferring value to another user is in possession of the private key capable of signing the transaction.

Private keys are generated by wallet software by executing a cryptographic hash function (*i.e.*, an algorithm) against a randomly generated number. Private keys are expressed as a long alphanumeric code and are used in cryptography similarly to a password. Effectively, private keys are used to authorize transactions and prove ownership of digital assets. A private key is an integral part of blockchain technology, and its encrypted properties help to protect a user from theft and unauthorized access to their digital assets. A private key is all that is required to authorize a transaction and therefore should be kept highly secure by its owner (or custodian).

Public keys identify the user's account and are created by executing a cryptographic hash function against the generated private key. Depending on the particular blockchain, public keys may then be hashed an additional time to generate a public key address (which is shorter than the public key). This public key address is what is publicly available on a blockchain, and most blockchain implementations make use of addresses as the "to" and "from" endpoints in a transaction. Users may be able to create multiple public keys from the same wallet, all being controlled by the same private key.

Both public and private keys are necessary to authorize and verify digital asset transactions. Private key holders can "sign" and authorize transactions by using their private keys to direct the associated wallets to "spend" digital assets. Public keys are used to direct this transaction to a designated recipient. The recipient will then use their own private key to decrypt and accept the transaction. Some of this process occurs "behind the scenes" by virtue of the technology. While users must affirmatively "sign" a transaction before it is broadcast to the blockchain network, users generally do not need to take any affirmative steps to receive a transaction. The process of designating a public address as the transaction recipient is very important. Blockchains generally do not verify that a designated address belongs to the intended recipient or that the address even exists. Digital assets sent to an incorrect or invalid address are generally irrecoverable.

There are different analogies used to describe public and private keys. A public key often is analogized to an email address, with the private key as the password for the corresponding email account. Email addresses (like public keys) are public and used to

identify senders and recipients. Passwords (like private keys) are kept private to prevent unauthorized access to information. Another common analogy is that public keys are like bank account numbers and private keys are like the associated account passwords.

Users must be focused on keeping their private keys secure and confidential because (1) any holder of a private key can "spend" digital assets by using the private key to direct the digital wallet to authorize a transfer of digital assets to another public key address and (2) critically, unlike with most email or bank account passwords, if a user loses a private key, then any digital asset associated with that key could be permanently lost. Possession of a private key grants any person control of the digital assets controlled by that wallet.

3. Introduction to Wallets

A digital wallet is "an application used to generate, manage, store or use private and public keys," which "can be implemented as a software or hardware module."[4] Wallets allow users to control and transfer digital assets to other users. Specifically, wallets serve to generate and store one's private keys. Wallets may also perform other functions, such as calculating a user's total number of digital assets.

Digital assets are intangible assets that are associated with a particular account or address on a blockchain ledger. Unlike physical wallets used for cash, digital wallets do not actually store or contain digital assets. Rather, digital wallets are an interface that allow for management of the public and private keys used to control digital assets on a blockchain network. Accordingly, unlike traditional custodians that may hold and safeguard assets in a vault or lockbox, DACs do not hold and safeguard digital assets, but rather hold and safeguard private keys necessary to control and transfer digital assets on a blockchain.

Because wallets are applications that interact with blockchain software, they must be compatible with the relevant blockchain. This means that not all wallets will be compatible with all types of digital assets. Certain wallets may be compatible with many types of digital assets; other wallets may be designed to be compatible only with a single type of digital asset.

a. Hot and Cold Wallets

One common method of describing and categorizing digital wallets is identifying them as "cold" or "hot."

"Cold" wallets are not connected to the internet and are physically isolated (*i.e.*, "air-gapped"). Examples of cold wallets include physical storage devices or other type of

[4] International Organization for Standardization (2020) *ISO 22739:2020 - Blockchain and distributed ledger technologies — Vocabulary* (Technical Committee 307). Available at https://www.iso.org/standard/73771.html.

hardware. This can be as simple as printing a private key on a piece of paper (often reflected as a QR code), or using hardware (e.g., USBs) or more sophisticated devices (e.g., hardware security modules). The main benefit of cold wallets is that, in certain ways, they provide higher levels of security and reduce the risk of hacking or improper copying. However, cold wallets may raise issues with having quick access to assets, creating liquidity concerns, and may cause other security concerns, such as physical theft or misplacement.

"Hot" wallets are generally categorized as private keys that are stored online. These require devices to be online in order to transfer assets. Examples of hot wallets include web-based wallets, mobile wallets, and desktop wallets. The main benefit of hot wallets is the ease of use and speed. As hot wallets are always online, they make transactions more efficient and accessible, and transactions may be automated with less need for human involvement. However, hot wallets are more susceptible to hacking and certain types security vulnerabilities.

Some wallet arrangements are referred to as "warm." Warm wallets generally mix hot and cold infrastructure, and, as such, refer to a *process* rather than purely a storage mechanism. For example, a warm wallet solution may have access to the internet, but require human intervention for further security.

As discussed in more detail below, all wallet solutions have drawbacks and advantages.

b. Additional Wallet Concepts

Beyond "hot" and "cold" wallets, which fundamentally refer to whether private keys are accessible via the internet, there are a number of other important technological, operational, and procedural concepts that impact private key management and usage.

At a high level, private key management encompasses the following:

1. **Key Generation**: the process of creating a private key.
2. **Key Storage**: the safekeeping of private key information.
3. **Key Usage**: the technological and procedural steps to control access and safeguard private key information when using private keys to effect digital asset transactions.

The following technologies are often used in institutional-grade custody solutions:

HSMs: As mentioned above, hardware security modules ("HSMs") are devices specially designed to create, store, and manage the use of private keys. HSMs generally are built to comply with recognized security standards.[5] Private keys typically cannot be copied or otherwise extracted from an HSM.

MPC: Multi-party computation ("MPC") is mathematical model that enables private keys to be generated and stored in "pieces," such that no single device contains the

[5] For example, many HSMs comply with U.S. Federal Information Processing Standard (FIPS) Publication 140-2, which defines minimum security requirements for cryptographic modules in information technology products.

entire private key. This offers additional protection against compromise/unauthorized access. However, MPC models may be limited by human error, including coding of the MPC function and logistical arrangements. The process of splitting a private key into multiple components is known as *sharding*, which process may or may not involve MPC.

Multisig: Multisig, or multi-signature, arrangements require more than one private key to authorize a transaction, similar in concept to requiring multiple signers on a bank account to effect a transaction.

C. Overview of Custodial Solutions

There is a wide array of custodial solutions available. Whether choosing to self-custody or utilize the services of a DAC, there are various wallet technologies that can be utilized, and one must balance considerations such as cost, efficiency, accessibility, and security.

1. Self-Custody or Noncustodial Wallets

The first option for digital asset custody is self-custody. Self-custody provides the owner with exclusive control of their private keys, rather than entrusting the keys to a third party. In this Section, we further discuss three primary wallet types that can be utilized for self-custody (as well as by DACs): paper wallets, hardware wallets, and software wallets. We also discuss a non-custodial wallet-as-a-service model.

a. Paper Wallets

The simplest form of wallet that can be utilized for self-custody is a "paper wallet," which stores the private keys entirely offline. Practically, a paper wallet is a piece of paper that contains public and private key information. To access one's digital assets, a user often will need a digital asset wallet application to scan a QR code and transfer the assets into the software wallet. In addition, users may need to take additional steps, such as creating a "change address" via "sweeping" the paper wallet, to ensure that their unused balances are not lost in transactions.

Paper wallets are relatively inexpensive and easy to generate. Generally, users can utilize a paper wallet generator website and print the corresponding paper wallet. However, users may choose to take additional steps to further secure their paper wallet, such as destroying the printer used to create the wallet, adding BIP 38 passwords to further encrypt their private key with a password, or taking steps to prevent potential malware risks from generating and printing their private key.

Paper wallets are an increasingly unpopular option, particularly in view of the emergence of other viable custody options. Holding large amounts of digital assets in a paper wallet presents complications. As paper is a physical medium, it is subject to

damage, fire, water, loss, and theft. If another user obtains the paper wallet, they would be able to access and spend the digital assets contained in the wallet with little or no recourse available to the genuine owner. Additionally, many popular digital assets simply do not support a paper wallet format.

b. Hardware and Cold Wallets

"Hardware" wallets may also be utilized for self-custody. A hardware wallet is a physical device that stores the user's private keys. The terms "hardware wallet" and "cold wallet" (described above) are sometimes used interchangeably, though there are distinctions. Hardware wallets keep private keys isolated from an internet connection. In this way, hardware wallets are designed to be extremely difficult to access by third parties, even when connected to a device that is connected to the internet. Hardware wallets accomplish this by signing transactions on the hardware device itself, broadcasting the transaction to the digital asset's ledger using a "crypto-bridge" to transfer unsigned transaction data to the hardware wallet, so that it can sign such data to the offline private keys.

Hardware wallets are considered one of the most secure ways to store digital assets, and there are a number of companies that specialize in building hardware wallets for DAC customers. However, if certain hardware wallets (along with any recovery phrases) are lost or destroyed, it may be difficult or impossible to difficult to recover the user's funds. For example, in 2013, an IT engineer lost 7,500 bitcoins after mistakenly disposing of a hard drive containing the cryptographic private keys needed to access and spend his bitcoins.[6]

However, hardware wallet options are continuing to evolve. For example, certain companies can now provide customers with a multi-sig recovery plan should they ever lose access to their hardware wallets. These firms offer "collaborative custody" solutions, where they function as authorized users of a minority number of private keys in a multi-signature wallet. Because the majority of the keys in a multi-sig arrangement is necessary to sign a transaction, the service provider cannot unilaterally cause digital assets to be spent from that address. However, a minority of keys in a multi-sig arrangement can be used to recover access to funds if a hardware wallet is lost or stolen.

c. Software Wallets

Software wallets can also be utilized for self-custody. Typically, software wallets store private keys within an interface that is connected to the internet, and are accessible through a web portal. In this way, software wallets are generally "hot" wallets. Given their internet connectivity, software wallets may be able to sign transactions and send transactions to the blockchain directly. Software wallets come in a variety of options.

---

[6]Ryan Browne, *Man Makes Last-Ditch Effort to Recover $280 Million in Bitcoin He Accidentally Threw Out*, CNBC (Jan. 16, 2021, 11:34 AM), www.cnbc.com/2021/01/15/uk-man-makes-last-ditch-effort-to-recover-lost-bitcoin-hard-drive.html.

For example, they may be integrated as browser extensions, desktop programs, and/or mobile applications.

Software wallets often allow users to access and transact with their digital assets easily and quickly. Additionally, software wallets often provide several accessibility options, given their iterations as software, desktop, or mobile applications. However, software wallets can pose certain security risks. As many software wallets are "hot" wallets, they may be more vulnerable to digital hacks than other wallet alternatives.

d. Non-Custodial "Wallet-as-a-Service"

Some companies are developing "wallet-as-a-service" models, which allow customer-facing businesses (e.g., digital asset exchanges) to embed a non-custodial wallet in their own applications. In this model, which may utilize MPC technology to divide private keys to multiple parties, customers maintain custody of their own digital assets, but the customer-facing business or the wallet-as-a-service company maintains the ability to recover the wallet. In addition to allowing for recovery, this model is designed to reduce "counterparty risk" to customers, by ensuring, for example, that assets are not comingled or rehypothecated by the customer-facing business.

2. Third-Party Custodians or Custodial Wallets

Generally, a custodial wallet is a wallet in which a third party manages the private key and maintains control over the user's wallet. Custodial wallets can vary widely with respect to scope of services offered, and some DACs incorporate analytics, trading, pricing, and valuation information into their platforms. In some circumstances, digital assets can be held in the custodian's name on a blockchain, allowing the custodian to operate these assets with proper permission from the customer.

Custodial wallets provide users with the convenience of having an external entity manage the security of their private keys. Users are not required to store and remember their private keys and, in the event of losing access to log-in credentials for the wallet, service providers have recovery options available. However, users must trust the service provider to take reasonable precautions to protect their assets from hacking and is otherwise operating the company in a responsible manner. Further, as users share their private keys with custodians, DACs may have the ability to freeze or restrict wallet access.

One popular form of custodial wallet is simply utilizing a wallet controlled by a centralized trading platform or custodial exchange. Custodial exchange wallets may exercise control and management of private keys, while allowing the customer to maintain access through an online portal. Exchange platforms often allow users to transfer digital assets to one another, combining wallet and exchange services.

When users utilize a custodial exchange wallet, they typically enter into a customer agreement with the custodial exchange. The legal relationship established by executing a customer agreement between a user and the custodial exchange varies. For example,

in certain instances, user agreements require that, to transfer digital assets to another, both transferor and transferee must hold digital assets in the custodial exchange's wallet.

To more efficiently custody assets, some exchanges may use a shared blockchain address, controlled by the exchange, to hold digital assets for its customers (sometimes referred to as an "omnibus" account). Retaining control of customers' private keys and commingling them in non-differentiated, asset-specific wallets has potential implications with respect to a customer's claim of ownership over digital assets held on the custodial exchange.

Although these platforms have been highly popular given their accessibility and ease of use, as is the case with all custody solutions, there are certain drawbacks. As an initial matter, users must trust the records and safekeeping of the exchanges. Users must also trust that the platforms are secure. Given that these exchanges have access to (and control over) private keys, any vulnerabilities could lead to a loss of the customer's assets.

Many exchanges offer customers various products and services that could potentially impact a customer's rights in digital assets that they "own," and alter the obligations owed by custodial exchanges to their customers. For example, staking-as-a-service (SaaS) is a popular way for custodial exchanges to generate income. Once a customer decides to stake their assets, customers will earn a yield on such digital assets that is paid by the custodial exchange. In this model, the exchange may lend the staked digital assets to a third party at a rate higher than the rate paid to customers. This arrangement can involve unsecured loans made by custodial exchanges to third parties. When assets are staked, assets may be commingled with other assets and may be deemed to be no longer held in trust.

Another variation of third-party custody is the use of licensed banking or bank-like institutions, such as state and federal-chartered trust companies. In October 2022, BNY Melon was became the first large U.S. Bank to begin offering digital asset custody, to select customers. With expanding institutional interest (and interest by the general public) in digital assets, many expect the use of these more traditional types of institutions to offer custody solutions in the coming years. However, in view of the current regulatory climate, discussed in more detail in Section E, adoption has been halting.

While some bank and bank-like institutions offer exchange services, many focus on offering secure and compliant custodial services. Given their traditional function, one natural option for digital asset custody is trust companies, which act as fiduciaries to hold and transfer assets. As the name implies, trust companies generally hold digital assets in trust, often not staking assets, and rely on servicing fees for holding customers' assets. By not staking assets, trust companies may reduce the risk of overleverage and

illiquidity.[7] In addition, these institutions have minimum capital requirements and limit the types of digital assets that can be held.

D. Operational and contractual considerations for recipients of custody services

As outlined in the discussion above, the custody of digital assets involves a variety of considerations—including technological, operational, and legal. It may be possible, however, to mitigate risks by conducting thorough due diligence on any DAC and thoughtfully negotiating the terms of service and other relevant agreements with a DAC.

Furthermore, beyond prudence and sound business judgment, certain persons may have legal and regulatory obligations to consider potential digital asset custody solutions and ensure that the chosen custody solution fulfils applicable requirements. For example, investment advisers, regardless of whether they are registered with the SEC and must comply with the Custody Rule, have a general duty of care arising out of their fiduciary duty of care to advisory clients (both under the Investment Advisers Act and state law).[8] Similarly, failure to exercise due care in selecting a DAC can expose a person to liability, particularly if the DAC will be responsible for custody of significant amount of an entity's assets.

The following discussion highlights certain issues that can be raised while conducting operational and contractual due diligence of DACs, along with examples of questions that may be asked. This is not intended to be an all-inclusive list and other issues may be relevant for specific custodial arrangements that are not provided here. Although this discussion references guidance and regulation applicable to certain DACs to illustrate considerations when vetting and choosing a custodian, a substantive discussion of the legal and regulatory obligations of DACs follows in Section E.

1. Security and technology

It is no surprise that the safekeeping of private keys is paramount to digital asset custody. However, given the variety of technology solutions available for key generation and management, it is likely that different DACs (even those of comparable size and sophistication) may employ different methods to manage and safeguard private keys. Persons seeking to engage a DAC should understand the technology

---

[7] *See* David Rodeck & Johanna Leggatt, *What Is Crypto Staking?*, FORBES: ADVISOR (Sept. 15, 2022, 12:02 PM), www.forbes.com/advisor/au/investing/cryptocurrency/what-is-crypto-staking/.

[8] See, *e.g.*, Safeguarding Rule at footnote 232, discussing an "adviser's fiduciary duty including its duty of care or duty of loyalty under the Advisers Act, which extends to the entirety of the adviser-client relationship."

solutions and relevant security procedures used by that DAC, and assess whether they are sufficient for the customer's particular needs.

The SEC's statement on *Custody of Digital Asset Securities by Special Purpose Broker-Dealers* (discussed further herein) provides instructive guidance for custodian due diligence, even if the assets to be custodied are not securities and the DAC being evaluated is not a broker-dealer. For example, a person evaluating a DAC's custody solution could ask to review the custodian's documentation to confirm whether the custodian has policies and procedures that address:

1. the on-boarding of a [digital asset] such that the [custodian] can associate the [digital asset] to a private key over which it can reasonably demonstrate [] possession or control;
2. the processes, software and hardware systems, and any other formats or systems utilized to create, store, or use private keys and any security or operational vulnerabilities of those systems and formats;
3. the establishment of private key generation processes that are secure and produce a cryptographically strong private key that is compatible with the distributed ledger technology and associated network and that is not susceptible to being discovered by unauthorized persons during the generation process or thereafter;
4. measures to protect private keys from being used to make an unauthorized or accidental transfer of a [digital asset] held in custody by the [custodian]; and
5. measures that protect private keys from being corrupted, lost or destroyed, that back-up the private key in a manner that does not compromise the security of the private key, and that otherwise preserve the ability of the [custodian] to access and transfer a [digital asset] it holds in the event a facility, software, or hardware system, or other format or system on which the private keys are stored and/or used is disrupted or destroyed.[9]

Even best-in-class technology solutions can be insufficient if a custodian falls victim to social engineering attacks (such as phishing), the custodian fails to follow its own procedures, or from simple human error. The case of a state-charted trust company that provided digital asset custody (and sub-custody) services, which filed for Chapter 11 bankruptcy protection in the summer of 2023, provides a cautionary example. According to the company's court filings, the company unintentionally provided customers seeking to deposit digital assets with a wallet address to a "legacy" wallet the company could no longer access or control, rendering all digital assets sent to that address effectively lost.[10] It appears that the technology devices needed to access the

---

[9] Securities and Exchange Commission, *Custody of Digital Asset Securities by Special Purpose Broker-Dealers* (Feb. 26, 2021, effective date Apr. 27, 2021), at 11630, www.federalregister.gov/documents/2021/02/26/2020-28847/custody-of-digital-asset-securities-by-special-purpose-broker-dealers.

[10] *Prime Core Technologies Inc.*, Docket No. 1:23-bk-11161 (Bankr. D. Del. Aug 14, 2023), Doc. 14 at p. 21.

decommissioned legacy wallets had been (seemingly inadvertently) kept by a former employee. The company stated that is has taken a number of actions to avoid the scenario from happing again, including "taking steps to restrict customer contributions to [decommissioned wallets] through direct customer communication," "making improvements to the Company's digital asset inventory procedures," and "improving employee off-boarding procedures," among other things.[11]

2. Funding and Trade Flows

The current market structure for digital assets may differ from traditional financial markets in certain respects, and in many ways, continues to evolve. As a result, the roles and responsibilities of various market service providers remains unstandardized, and service providers may or may not provide the services that participants in traditional markets would expect or assume. Furthermore, regulatory requirements and uncertainty related to the treatment of digital assets may result in complex or non-standard funding arrangements and trade flows.

As just one example, on September 25, 2020, the SEC's Division of Enforcement issued a no-action letter to FINRA regarding the availability of noncustodial business models for broker-dealers transacting in digital asset securities.[12] The letter was in response to an inquiry from FINRA which noted that several broker-dealers seeking to operate an alternative trading system ("ATS") that trades digital asset securities had asserted that the "four-step process" previously described in the SEC and FINRA's *Joint Staff Statement on Broker-Dealer Custody of Digital Asset Securities*[13] increased operational and settlement risks.

The "four-step process" for broker-dealers operating an ATS described in the Joint Staff Statement involves:

> Step 1 – the buyer and seller send their respective orders to the ATS;
>
> Step 2 – the ATS matches the orders;
>
> Step 3 – the ATS notifies the buyer and seller of the matched trade; and
>
> Step 4 – the buyer and seller settle the transaction bilaterally, either directly with each other or by instructing their respective custodians to settle the transaction on their behalf.

---

[11] *Id.* at p. 23.

[12] Letter from Elizabeth Baird, Deputy Dir., Div. of Trading & Mkts, SEC, to Kris Dailey VP, Risk Oversight and Operations, FINRA (Sept. 25, 2020), available at https://www.sec.gov/divisions/marketreg/mr-noaction/2020/finra-ats-role-in-settlement-of-digital-asset-security-trades-09252020.pdf.

[13] Division of Trading and Markets, SEC, and Office of General Counsel, FINRA, Joint Staff Statement on Broker-Dealer Custody of Digital Asset Securities, (Jul. 8, 2019) available at https://www.sec.gov/news/public-statement/joint-staffstatement-broker-dealer-custody-digital-asset-securities (the "Joint Staff Statement").

In response to FINRA's inquiry, the SEC, while maintaining the availability of the four-step process, stated it would also permit a "three-step process" for broker-dealers operating an ATS (provided that additional requirements described in the no-action letter are met):

> Step 1 - the buyer and seller send their respective orders to the ATS, notify their respective custodians of their respective orders submitted to the ATS, and instruct their respective custodians to settle transactions in accordance with the terms of their orders when the ATS notifies the custodians of a match on the ATS;
>
> Step 2 - the ATS matches the orders; and
>
> Step 3 - the ATS notifies the buyer and seller and their respective custodians of the matched trade and the custodians carry out the conditional instructions.

Although this example relates only to specific use cases involving digital asset securities (as opposed to other types of digital assets), it illustrates the ways various parties may be responsible for providing settlement instructions to a DAC depending on agreed upon roles and responsibilities.

Similarly, SEC staff recently stated, "[the SEC] understand[s], much of [] crypto asset trading volume occurs on crypto asset trading platforms that often directly settle the trades placed on their platforms. As a result, many crypto trading platforms require investors to pre-fund trades, a process in which investors transfer their crypto assets, including crypto asset securities, or fiat currency to such an exchange prior to the execution of any trade."[14] Because the SEC believes many digital asset trading platforms do not meet the definition of a qualified custodian (either under the proposed Safeguarding Rule or existing Custody Rule), this would not be a compliant trade flow for registered investment advisers trading client assets. However, the SEC goes on in the Safeguarding Rule proposing release to ask a number of questions about the availability of alternative trade flows, including those facilitated by technology (e.g., "atomic swaps"), as well as potential arrangements between customers, custodians, and other parties that may be contractually agreed upon.[15] Accordingly, persons seeking to engage a DAC should explore what potential funding and trade flow models are supported by the DAC (and other parties that would be involved in the various stages of clearance and settlement, such as any trade execution venues) that would meet the customer's regulatory and business needs. This allocation of responsibilities should be clearly described in contractual agreements.

---

[14] SEC Release No. IA-6240, https://www.sec.gov/files/rules/proposed/2023/ia-6240.pdf (the "Safeguarding Rule"), at 14689.

[15] *Id.*

3. Common Contractual Provisions and Risk Allocation

Contractual terms may have important implications in the context of a DAC insolvency. In the Chapter 11 cases of digital asset platform Celsius Network LLC and its affiliates (Celsius), the presiding bankruptcy court found the Terms of Use accepted by Celsius account holders were unequivocally clear that the title to and ownership of digital assets deposited by customers into "Earn" accounts were transferred to Celsius, and Celsius had full rights to use and invest those assets. [16] It is important to note that the court's ruling did not address the digital assets held under Celsius' "Custody" or other programs, each of which is the subject of separate disputes and litigation. Account holders can be bound by such terms even if they did not read or fully appreciate the consequences of the terms. As such, it is important for blockchain market participants to be thoughtful about the language in any digital asset customer agreements, including the choice of law provision, and any related marketing materials, but particularly differences in terms for different product offerings.

While the bankruptcy court in Celsius found that the contract language on title transfer and ownership was dispositive to determining that the digital assets at issue were property of the estate, it is important to recognize that the contract language may not be dispositive in all contexts, particularly if a party is seeking to exclude assets from a bankruptcy estate. Other factors include, among other things, whether the assets to be excluded have been commingled with estate property and whether a party can trace those assets following such commingling.[17] Further, as a practical matter, Celsius had a significant shortfall in the amount and types of digital assets it was holding for Earn account holders, so it would not be possible for Celsius to return the digital assets to each account holder even if the contract terms provided that the Earn account holders retained ownership of the digital assets. Market participants should therefore be mindful of practical, as well as legal, risks of digital asset investing.

However, persons seeking DAC services may seek to address such issues through contract (provided a DAC is willing and able to agree to such terms). For example, it may be possible to specify by contract whether the customer's digital assets will be

---

[16] In re Celsius Network LLC, Case No. 22-10964 (Bankr. S.D.N.Y. Jan. 4, 2023), Memorandum Opinion and Order Regarding Ownership of Earn Account Assets, Docket No. 1822. *See also* Sidley Austin LLP, *Celsius Bankruptcy Court Confirms That Customer Digital Assets Are Property of the Estate in Key Ruling* (Jan. 17, 2023) https://www.sidley.com/en/insights/newsupdates/2023/01/celsius-bankruptcy-court-confirms-that-customer-digital-assets-are-property-of-the-estate.

[17] For example, in the Bankruptcy Court's December 20, 2022, order addressing certain of the digital assets held under the Custody program, the Bankruptcy Court declined to find that the digital assets that were held for Custody accounts but that were not held in the segregated Custody wallet were not property of the estate and instead reserved on that issue for further proceedings. See Docket No. 1767. While Celsius argued that the Terms of Use provide that title and ownership of the digital assets in the Custody program are not property of the estate regardless of where such assets were stored, the creditors' committee's position is that only digital assets held in the segregated Custody wallet should be excluded from the estates. See, *e.g.*, *Debtors' Responsive Brief on Phase I Custody and Withhold Issues*, Docket No. 1567 (Dec. 2, 2022).

segregated or commingled with the custodian's proprietary assets, or assets of other customers. Similarly, it may be possible to address by contract what ownership rights the custodian has with respect to customers' assets. For example, will the custodian be able to sell, lend, rehypothecate, or grant a security interest in custodial assets? Will the Uniform Commercial Code apply to the custodial account (and would there be any carve outs)?

Even outside of an insolvency context, an asset shortfall may arise (e.g., in the event of a hack, theft, or other loss). It may be possible to specify how such shortfalls will be addressed in the contract for custodial services. For example, will the DAC have insurance that covers losses of custodial assets for the benefit of customers? If so, what are the coverage limits and exclusions? If losses exceed coverage amounts, how will the policy be apportioned among customers?

The SEC's proposed Safeguarding Rule also provides instructive guidance on important contractual provisions for custodial relationships, even if the customer is not a registered investment adviser (and even if the rule is not adopted as proposed). The proposed Safeguarding Rule would require certain registered investment advisers to obtain reasonable assurances in writing (that is, by contract) that "minimum custodial protections" will be provided.[18] Those fundamental protections outlined in the proposed Safeguarding Rule include:

- A qualified custodian should exercise due care and implement appropriate measures to safeguard the advisory client's assets;
- A qualified custodian should indemnify an advisory client when its negligence, recklessness, or willful misconduct results in that client's loss;
- A qualified custodian should not be relieved of its responsibilities to an advisory client as a result of sub-custodial arrangements;
- A qualified custodian should clearly identify an advisory client's assets and segregate an advisory client's assets from its proprietary assets;
- The client's assets should remain free of liens in favor of a qualified custodian unless authorized in writing by the client;
- A qualified custodian should keep certain records relating to those assets;
- A qualified custodian should cooperate with an independent public accountant's efforts to assess its safeguarding efforts;
- Advisory clients should receive periodic custodial account statements directly from the qualified custodian;

[18] Safeguarding Rule at 14690-14691.

- A qualified custodian's internal controls relating to its custodial practices should be evaluated periodically for effectiveness; and
- A custodial agreement should reflect an investment adviser's agreed-upon level of authority to effect transactions in the advisory client's account.[19]

It is important that any person selecting a custody solution know what software and hardware systems will be used, and understand any potential advantages and disadvantages of each system as applied to that person's own context and needs. Equally important to any technology solution however, are the operational policies and procedures a custodian should implement, maintain and follow to ensure that keys are protected as intended. There may be circumstances when specific protections listed above are less applicable to a particular custodial relationship, and the customer and custodian may reasonably make trade-offs when negotiating a custodial agreement depending on additional factors (such as cost). Nonetheless, considering whether and how these elements are addresses in a custodial relationship may be a constructive exercise.

E. Regulatory Considerations

As described above, digital asset custody is an evolving and growing service. This section discusses various legal and regulatory obligations that may be applicable to custodial arrangements.

In the United States, the regulatory landscape is complex. Particularly because of the unsettled and shifting environment, regulatory considerations pose unique challenges for DACs. There is a wide variety of regulations and laws that are potentially applicable to DACs. Here we focus on four key bodies of regulation: (i) investment adviser regulations (including the Custody Rule), (ii) broker-dealer regulations (including the Customer Protection Rule), (iii) banking regulations, and (iv) various other state and federal laws and regulations (including BSA and AML obligations).

1. Investment Advisers and the Custody Rule

Investment advisers are subject to Rule 206(4)-2 under the Investment Advisers Act of 1940, as amended (the "Custody Rule"). Generally, an investment adviser is (i) a firm or person (ii) that, for compensation, engages in (a) the business of providing investment advice to others about the value of or about investing in securities and/or (b) issuing reports or analyses regarding securities as part of a regular business.[20]

---

[19] *Id. at* 14693.

[20] U.S. Code, Title 15, Chapter 2D, Subchapter II, Section 80b-2(a)(11); U.S. Securities and Exchange Commission, *Investment Adviser* (Sept. [_], 2023), www.investor.gov/introduction-investing/investing-basics/glossary/investment-

Investment advisers registered with the Securities and Exchange Commission (the "SEC") are subject to the Custody Rule.

Of course, the issue of whether a digital asset is a security or sold as part of an investment contract – and therefore as part of a securities transactions – is a complex and unsettled. The SEC has taken the position that many digital assets are sold in "securities transactions," and there are many matters pending in the courts and pieces of legislation pending before Congress that could have a dramatic impact on the regulatory classification of digital assets.

The Custody Rule imposes additional regulatory requirements when an adviser has "custody" of a client's assets. Custody generally "means holding, directly or indirectly, client funds or securities, or having any authority to obtain possession of them,"[21] and can include arrangements where the adviser has "deemed" custody.

One of the requirements of the Custody Rule is that when an adviser has custody of its client's fund and securities, those assets, including "digital asset securities", must be held with a qualified custodian. Generally, a qualified custodian includes broker-dealers, banks, savings associations, transfer agents, and certain foreign institutions. In addition, such client assets would need to be maintained either (i) in a separate account for each client under that client's name or (ii) in accounts that contain only the adviser's clients' funds and securities, under the adviser's name as agent or trustee for its clients.[22] Thus, SEC registered investment advisers with custody of their clients' assets should ensure that their clients' assets are being held with a qualified custodian in accordance with the Custody Rule.

The Custody Rule requires that investment advisers take specific compliance steps. For example, investment advisers may need to provide notice to their clients if an account is opened with a qualified custodian on those clients' behalf. The investment adviser may need to send – or have the reasonable belief that the qualified custodian will send – account statements to its clients at least quarterly. In addition, the Custody Rule may require that investment advisers are subject to verification procedures, generally at least once during any calendar year, by an independent public accountant and subject to surprise audits.

The requirements of complying with the Custody Rule have raised issues for investment advisers custodying digital assets. Although the SEC has stated that "most crypto assets are likely to be funds or crypto assets securities covered by the current [Custody Rule],"[23] there has been confusion as to whether the Custody Rule in fact covers all digital assets. Moreover, the Custody Rule raises practical compliance

---

adviser#:~:text=An%20investment%20adviser%20is%20a,and%20certain%20other%20investment%20products.

[21] Title 17, Chapter II, Part 275, Section 275.206(4)-2(d)(2), https://www.ecfr.gov/current/title-17/part-275/section-275.206(4)-2#p-275.206(4)-2(d)(2).

[22] *Id.*

[23] *See* Chair Gary Gensler, Statement on Proposed Rules Regarding Investment Advisor Custody (Feb. 15, 2023).

difficulties. For example, custodying digital assets with a qualified custodian and verifying that the assets are being held in custody can be a difficult technological question. In addition, creating and providing audited financial statements in the changing digital asset space may be difficult for traditional accounting firms, given potential fluctuations of digital assets.[24]

Recent proposed changes to the Custody Rule to expand its scope as the "Safeguarding Rule" have further amplified these concerns.[25] On February 15, 2023, the SEC issued a proposed rule to significantly amend and replace the Custody Rule with the "Safeguarding Rule."[26] Beyond the change in nomenclature, the proposed Safeguarding Rule provides significant changes that would affect the digital asset industry.

First, the proposed Safeguarding Rule expands the Custody Rule's scope to apply to all customer assets over which a registered investment adviser has custody, including "other positions held in a client's account that are not funds or securities."[27] As stated in the proposal, this would include all types digital assets, even in instances where such assets are neither funds nor securities.[28] Thus, under the proposed Safeguarding Rule, investment advisers with custody over their client's digital assets would explicitly need to comply with the heightened Safeguarding Rule requirements.

Second, the proposed Safeguarding Rule significantly increases the requirements for investment advisers and qualified custodians. The Safeguarding Rule increases certain qualified custodian requirements, such as: (i) providing heightened requirements for foreign financial institutions, (ii) stating that qualified custodians would need to participate in any change in beneficial ownership of assets and effectuate transactions, and (iii) requiring registered investment advisers to enter into written agreements with the qualified custodian regarding due care, indemnification, and segregation of client assets.

Third, the proposed Safeguarding Rule also provides further requirements regarding segregation of customer assets and recordkeeping. With regard to segregation of client assets, the Safeguarding Rule provides that customer assets: (i) must not be commingled with the adviser's assets or its related person's assets, (ii) must be titled or registered in the customer's name or otherwise held for benefit of that customer, and (iii) must not be subject to any right, charge, security interest, lien or claim of any kind in favor of the adviser, its related persons, or its creditor, unless agreed to or authorized in writing by the client. Regarding the surprise examination

---

[24] Amanda Gould, *Crypto Custody* (Aug. [_], 2023), www.law.upenn.edu/faculty/david-hoffman/crypto-custody.php.

[25] Winston & Strawn, LLP, *SEC Proposes New Safeguarding Rule to Replace Custody Rule, With Widespread Implications* (Mar. 6, 2023), www.winston.com/en/thought-leadership/sec-proposes-new-safeguarding-rule-to-replace-custody-rule-with-widespread-implications.html.

[26] SEC Release No. IA-6240, https://www.sec.gov/files/rules/proposed/2023/ia-6240.pdf (the "Safeguarding Rule").

[27] The Safeguarding Rule, at 27.

[28] *Id. at* 28.

requirements, the registered investment adviser must "reasonably believe" that a written agreement has been implemented with an accountant, *i.e.*, that an accountant will perform the surprise examination, and that notice of any material discrepancies will be sent to the SEC.

Following the SEC's release of the Safeguarding Rule proposal, the SEC has continued to issue guidance that raises further inquiries. For example, in July 2023, the SEC released a statement from Paul Munter, the SEC's Chief Accountant, regarding accounting firms and digital assets.[29] In his statement, Munter emphasizes that accounting firms "must keep several obligations and hazards front of mind." Specifically, accounting firms should "carefully consider the contents of any statements" given potential antifraud violations. In addition, accounting firms should reconsider their engagement with "new entrants to the crypto industry" with lack of a track record, and potentially implement "certain precautions." These accounting principles are especially critical in Custody Rule compliance, given the requirements for audited financial statements and surprise inspections. As a result, it is clear that further scrutiny is being taken by the SEC regarding custody requirements of digital assets.

2. Securities Broker-Dealers, the Exchange Act, and the Customer Protection Rule

Along with many registered investment advisers, the SEC oversees the securities markets generally and regulates platforms or exchanges that are federal broker-dealers.[30] To be classified as a securities "broker-dealer" under the Exchange Act, an entity or person must be "engaged in the business of effecting transactions in securities for the account of others."[31] This includes facilitating the issuance of security tokens and secondary trading in securities. Because broker-dealers are afforded some agency over their customers' assets, they are required to register with the SEC, become a member of the self-regulatory organization FINRA, and meet certain financial responsibility requirements.

Broker-dealers must comply with the applicable custodial requirements under Rule 15c3-3 of the Exchange Act, known as the "Customer Protection Rule."[32] The Customer Protection Rule details broker-dealer capital requirements and is designed to safeguard customer securities and funds held by a broker-dealer, prevent investor loss in the event

---

[29] U.S. Securities and Exchange Commission, Paul Munter, *The Potential Pitfalls of Purported Crypto "Assurance" Work* (July 27, 2023), www.sec.gov/news/statement/munter-statement-crypto-072723?utm_medium=email&utm_source=govdelivery.

[30] 15 U.S.C. 77e.

[31] 15 U.S.C. § 78c(a)(4)(A) (2012).

[32] SEC, Division of Trading and Mkts and FINRA, Off. Of Gen. Couns., *Joint Staff Statement on Broker-Dealer Custody of Digital Asset Securities* (July 8, 2019), accessed August 1, 2023, https://www.sec.gov/news/public-statement/joint-staff-statement-broker-dealer-custody-digital-asset-securities.

of a broker-dealer's failure, and enhance the SEC's ability to monitor and prevent unsound business practices. Generally, the Customer Protection Rule requires brokers to promptly obtain and, thereafter, maintain possession or control over customers' fully paid securities and/or excess margin securities.

In April 2021, the SEC issued a statement regarding the Custody of Digital Asset Securities by Special Purpose Broker-Dealers ("SPBDs").[33] SPBDs are financial institutions that operate within the securities industry and have been authorized by the SEC to engage in specific activities or cater to particular types of securities. The 2021 statement, which is effective for five years, provides a set of nine requirements that SPBDs operating in the digital asset space must meet in order to remain compliant with the Customer Protection Rule.[34] Those requirements are summarized as follows:

1. The broker-dealer has access to the digital asset securities and can transfer these securities using distributed ledger technology;
2. The broker-dealer focuses on activities solely related to digital asset securities, such as dealing, transaction execution, custody, and operating an alternative trading system. The broker-dealer can hold and trade traditional securities only for its own account to meet Net Capital requirements per Rule 15c3-1 of the Exchange Act.
3. The broker-dealer establishes, maintains, and enforces policies and procedures to analyze whether a digital asset security has met relevant registration or exemption requirements, and the broker-dealer ensures compliance with federal securities laws for transactions and custody.
4. Before—and periodically after—taking custody of a digital asset security, the broker-dealer evaluates the characteristics of the associated distributed ledger technology and its network.
5. The broker-dealer refrains from custodying a digital asset security if there are significant security or operational issues with the associated distributed ledger or if it poses material risks to the broker-dealer's business.
6. The broker-dealer establishes, maintains, and enforces policies and procedures aligned with industry best practices to maintain exclusively control over digital asset securities and protect against theft, loss, and unauthorized use of private keys.
7. The broker-dealer establishes, maintains, and enforces policies and procedures for various events that could impact custody, including blockchain malfunctions, 51% attacks, hard folks, or airdrops. It also allows compliance with court-ordered freezes or seizures and facilitates the transfer of digital asset securities to appropriate entities during self-liquidation or bankruptcy.

---

[33] Securities and Exchange Commission, *Custody of Digital Asset Securities by Special Purpose Broker-Dealers* (Feb. 26, 2021, effective date Apr. 27, 2021), www.federalregister.gov/documents/2021/02/26/2020-28847/custody-of-digital-asset-securities-by-special-purpose-broker-dealers.
[34] *Id.* at 11631.

8. The broker-dealer provides written disclosures to customers, informing them that the firm considers itself in possession or control of digital asset securities. It also highlights risks associated with investing in or holding digital asset securities, including limited protections under the Securities Investor Protection Act ("SIPA"), fraud, manipulation, theft, valuation, volatility, liquidity, and security protocols. The broker-dealer is not expected to disclose specific security protocols, but disclosures should emphasize how security measures safeguard the broker-dealer's private keys against loss, theft, or unauthorized or accidental use.
9. The broker-dealer enters into written agreements with customers, outlining terms and conditions for various activities related to digital asset securities, such as receiving, purchasing, holding, selling, transferring, custodying, and liquidating.

SPBDs must comply with the regulatory requirements imposed by regulators such as FINRA and the SEC.[35] SPBDs, like traditional broker-dealers, are required to maintain accurate and timely financial records, submit regular financial reports, and demonstrate compliance with the Financial Responsibility Rules (including the Customer Protection Rule), thereby promoting transparency and protecting customers in the evolving digital asset landscape. Additionally, broker-dealers planning to facilitate secondary market transactions of digital assets are likely to face unique challenges based on the many types of digital assets. These challenges are the cause for uncertainty in how current regulations will evolve.

In a controversial March 2022 Staff Account Bulletin ("SAB 121"), the SEC stated that in view of the "unique risks and uncertainties" any entity responsible for safeguarding digital assets should "present a liability on its balance sheet to reflect its obligation to safeguard the crypto-assets held for its platform users."[36] Such a custodian is required to include clear disclosures in their financial statements to their customers of the nature and amount of digital assets that the exchange is responsible for holding. SAB 121 also provides that a custodian may need to include further disclosures outside of financial statements (e.g., description of business, risk factors, or management's discussion and analysis of financial condition and results of operation), such as: (1) a description of types of losses or additional obligations that could occur (e.g., regulatory enforcement actions, litigation, or customer discontinuation), (2) an analysis of legal ownership of the digital assets held for platform users (e.g., satisfaction of general credit claims in event of bankruptcy), and (3) the potential impact that the unavailability of cryptographic key information would have on the custodian (including risk-mitigation steps).

In October 2023, the U.S. Government Accountability Office concluded that SAB 121 is a "rule" for purposes of the Congressional Review Act (the "CRA"), such that it is

[35] FINRA approved Prometheum Ember Capital as the first SPBD allowed to custody digital asset securities on behalf of its customers on May 17, 2023.
[36] SEC Staff Accounting Bulletin No. 121, 17 Fed. Reg. 211 (Mar. 31, 2022).

subject to Congressional Review.[37] Shortly thereafter, a bipartisan group of members of Congress authored a letter to the prudential regulators calling into question the enforceability SAB 121, asserting that the approach proposed by the SEC "deviates from established account standards," "would not accurately reflect the underlying legal and economic obligations of the custodian, and places consumers at greater risk of loss."[38] The letter states that because SAB 121 did not meet the relevant procedural review requirements, it "should have no legal effect" and is unenforceable.

While the enforceability of SAB 121 remains unclear at the time of this writing, it remains a significant document given that it reflects aspects of SEC's current thinking about digital asset custody, and provides considerations for a custodiam as it develops its legal, regulatory, and accounting practices.

3. Prudential Banking Regulators

Banks have historically provided safekeeping and custody services for a variety of different financial instruments. A number of key prudential banking regulators have commented on the appropriateness of regulated banking institutions participating in the custody of digital assets.

In July 2020, the Office of the Comptroller of Currency, which charters, regulates, and supervises all national banks and savings associations – as well as federal branches and agencies of foreign banks – issued Interpretative Letter 1170, which concluded that "national banks may provide . . . cryptocurrency custody services on behalf of customers, including by holding the unique cryptographic keys associated with cryptocurrencies."[39] In its letter, the OCC recognized that safekeeping functions "are well established and extensively recognized as permissible activities for national banks," and that providing digital asset custody services, including safeguarding cryptographic keys, is essentially a modern form of those traditional services.[40]

In November 2021, the OCC's Chief Counsel issued Interpretive Letter 1179, purporting to "clarify" Interpretive letter 1170 and two other letters relating to digital assets.[41] In Interpretive Letter 1179, the OCC takes the position that custodial and other services for digital assets are legally permitted, "*provided* the bank can demonstrate, to the satisfaction of its supervisory office, that it has controls in place to conduct the activity in a safe and sound manner."[42] The OCC reasoned that if a bank lacks the capacity to provide digital asset custodial services in a "safe and sound manner," the

---

[37] U.S. Government Accountability Office, Securities and Exchange Commission – Applicability of the Congressional Review Act to Staff Accounting Bulletin No. 121, https://www.gao.gov/products/b-334540.

[38] Letter from Congressman Patrick McHenry, et al, to FDIC, et al (Nov. 15, 2023), https://financialservices.house.gov/news/documentsingle.aspx?DocumentID=409042.

[39] Office of the Comptroller of Currency, Interpretive Letter 1170 (July 22, 20220.

[40] *Id.*

[41] Office of the Comptroller of Currency, Interpretive Letter 1179 (Nov. 18, 2021).

[42] *Id.*

activity "cannot be part of the 'business of banking,' and therefore is not a permissible activity."[43] The upshot of the Interpretive Letter is that if a national bank wishes to engaged in digital asset-related activities, it must first notify the supervisory office in writing of its intentions and receive written non-objection before commencement of the activities. The bank must demonstrate that it has adequate risk management systems and controls in place to identify, measure and monitor the risks – including operational, liquidity, strategic, and compliance risks – of the contemplated activities.

The Federal Deposit Insurance Corporation ("FDIC"), an independent agency created to maintain stability in the financial system that insurers deposits as serves as the primary federal regulator of state-chartered banks that do no join the federal reserve system, issued a similar letter in April 2022, requiring the institutions it supervises to notify the FDIC of "activities involving or related to crypto assets."[44] Financial institutions are required to provide the FDIC Regional Director with a detailed description of the proposed activity, and provide the proposed timeline for engaging in the activity. The FDIC will then request additional information "as needed," and "consider the safety and soundness, financial stability, and consumer protection considerations" – and then "provide relevant supervisory feedback . . . as appropriate, in a timely manner."[45]

For their part, a variety of states have provided guidance relevant to digital asset custody. For example, since 2015, the New York Department of Financial Services has offered a "limited purpose rust company" charter for institutions solely focused on custodial services for digital assets. And in 2019, the Wyoming Division of Banking created the "Special Purpose Depository Institution" charter, specifically catering to firms facilitating digital asset transactions and custody. Other state regulators, like the Florida Office of Financial Regulation in 2022, issued guidance for Florida state-chartered financial institutions that Florida's Financial Institutions Codes do not prohibit state-charted financial institutions from providing virtual currency services to their customers, including custody services."[46]

State-charted banks that are members of the Federal Reserve System are also regulated by the Board of Governors of the Federal Reserve System (the "FRB"). In January 2023 (with an effective date of February 7, 2023), the FRB issued a policy statement designed to "level the competitive playing field among banks with different charters" (the "Policy Statement").[47] In the Policy Statement, the Fed "reiterate[d] . . .

---

[43] *Id.*

[44] FDIC, FIL-16-2022, Notification and Supervisory Feedback Procedures for FDIC-Supervised Institutions Engaging in Crypto-Related Activities (Apr. 7, 2022).

[45] *Id.*

[46] OFR, Guidance to Florida State-Chartered Financial Institutions Regarding the Provision of Virtual Currency and Digital Asset Custody Services (Jan. 2022).

[47] 12 C.F.R. § 208.112. The Policy Statement was released shortly after a January 3, 2023, Joint Statement by the Fed, the FDIC, and OCC issued a joint statement on crypto-asset risks to banking organizations, highlighting "key risks associated with crypto-assets and the crypto-asset sector participants." In the Joint Statement, the regulators emphasized that "[b]anking organizations should ensure appropriate risk

that legal permissibility is a necessary, but not sufficient, condition to establish that a state member bank may engage in a particular activity." While the FRB stated that it would "presumptively prohibit state member banks from holding digital assets as principal," it also noted that "nothing in the policy statement would prohibit a state member bank, or an applicant to become a state member bank, once approved, from providing safekeeping services for crypto-assets in a custodial capacity if such activities are conducted in a safe and sound manner and in compliance with consumer, anti-money-laundering, and anti-terrorist-financing laws."[48] State member banks and applicants should expect heightened scrutiny if they seek to offer digital asset custodial services; however, such activities are not without precedent. Several months before issuance of the Policy Statement, BNY Melon, the oldest bank in the United States, which is regulated by the Fed (as well as the New York State Department of Financial Service), launched its digital custody platform, allowing select clients to safeguard their bitcoin and other holdings.

4. Other Federal and State Laws and Regulations

A DAC may also be required to be licensed as a "money transmitter" at the federal level, as well as a "money services business" in the states in which it operates or has customers, giving rise to a variety of regulatory obligations. In the United States, at the federal level, digital asset businesses (including digital asset custodial exchanges) that are in the business of transferring virtual currencies often are deemed to be "money transmitters" and required to register with a division of the United States Treasury Department, the Financial Crimes Enforcement Network ("FinCEN"), that administers the Bank Secrecy Act (P.L. 91-508) (the "BSA").[49] Businesses that are considered "money transmitters" are referred to as money services businesses ("MSBs") and subject to anti-money laundering ("AML") and countering the financing of terrorism ("CFT") obligations under the BSA.

---

management, including broad oversight, policies, procedures, risk assessments, controls, gates and guardrails, and monitoring, to effectively identify and manage risks."

[48] 12 C.F.R. § 208.112.

[49] An administrator or exchanger that (1) accepts and transmits a convertible virtual currency or (2) buys or sells convertible virtual currency for any reason is a money transmitter under FinCEN's regulations, unless a limitation to or exemption from the definition applies to the person. FinCEN's regulations provide that whether a person is a money transmitter is a matter of facts and circumstances. The regulations identify six circumstances under which a person is not a money transmitter, despite accepting and transmitting currency, funds, or value that substitutes for currency. 31 CFR § 1010.100(ff)(5)(ii)(A)-(F). FinCEN requires certain businesses engaged in obtaining, distributing, exchanging, accepting, or transmitting virtual currencies to register as "money services businesses." JP Koning, *Let's Stop Regulating Crypto Exchanges Like Western Union*, NASDAQ.COM (November 22, 2022, 4:31 AM), https://www.nasdaq.com/articles/lets-stop-regulating-crypto-exchanges-like-western-union.

Although third-party exchanges may be required to comply with various FinCEN, BSA, AML and CFT obligations, their customers may not benefit from protections provided by the SIPC for holding registered securities or the FDIC for holding cash deposits. Moreover, it is not clear that any provider of hard wallet or cold wallet software for individuals to custody their own digital assets are subject to any state or federal government oversight based on certain exemptions that apply.

Recent foreign conflicts and stated fears of regulatory evasion using digital assets[50] have led to pushes for further sanctions and heightened procedures that could affect DACs. For example, in response to increased sanctions against Russian nationals, some exchanges and DACs adopted new KYC anti-money laundering measures.[51] These heightened policies come after increased pressure by government officials to investigate potential links to sanctioned countries and evasion attempts. Such pressure and investigation has led to investigations of exchanges, platforms, and DACs on these points. For DACs, compliance with sanctions is necessary and important. To that end, DACs may face increased scrutiny, expenses, and requirements to ensure compliance.

In addition, many DACs in the United States are regulated by state laws. For example, under the laws and regulations of many states, many digital asset businesses are required to adhere to rules and regulations set forth by the states in which they operate (and often where they have customers) and are subject to regular audits and inspections by state-government agencies.[52] Such businesses may also be required to be licensed, at the state level, as MSBs, which can impose certain safety, soundness, and customer protection requirements.

Attention should be paid to evolving state regulatory landscape, which is likely to impose new requirements on custodians. For example, amendments to the Uniform Commercial Code proposed in 2022 (the "2022 UCC Amendments") that address digital assets were adopted in May 2023.[53] The 2022 UCC Amendments add a new Article 12, covering new classes of property that include digital assets, and provides revisions to Article 9, requiring new methods for perfection and control, and new requirements for

---

[50] Congressional Research Service, Russian Sanctions and Cryptocurrency (May 4, 2022); Congressional Research Service, Russia Sanctions and Cryptocurrencies: Policy Issues (May 26, 2022). .

[51] Congressional Research Service, Russia Sanctions and Cryptocurrencies: Policy Issues (May 26, 2022).

[52] *See Enhancing Trust with Regulatory Compliance*, COINBASE, help.coinbase.com/en/coinbase/other-topics/legal-policies/enhancing-trust-with-regulatory-compliance (last visited Jan. 8, 2023); *Is Gemini Licensed and/or Regulated?*, GEMINI, support.gemini.com/hc/en-us/articles/204734485-Is-Gemini-licensed-and-or-regulated- (last visited Jan. 8, 2023); *Is Kraken Licensed or Regulated*, KRAKEN, support.kraken.com/hc/en-us/articles/360031282351-Is-Kraken-licensed-or-regulated- (last visited Jan. 8, 2023).

[53] Uniform Law Commission, 2022 Amendments to UCC Commercial Law & Finance. Available at https://www.uniformlaws.org/committees/community-home?communitykey=1457c422-ddb7-40b0-8c76-39a1991651ac#:~:text=The%202022%20amendments%20to%20the,intelligence%2C%20and%20other%20technological%20developments.

enforceability and priority.[54] Importantly, under the 2022 UCC Amendments, access to the private key associated with a digital wallet will determine control for purposes of perfection. As described above, certain customer agreements entered into between user and custodial exchange will have users agreeing to the custodial exchange retaining control over all private keys. This type of outsourcing of responsibility to hold private keys may have legal ramifications under the UCC for purposes of ownership and control.

More generally, several states have begun proposing comprehensive reforms regarding DACs, which should be monitored closely, as it could create further legal constraints and requirements on DACs and their customers.

F. Conclusion

As the digital asset sector continues to mature and gain prominence, and as technology continues to evolve and develop, so too will the types of services provided by DACs. It is important to stay apprised of the latest technical, operational, regulatory and legal developments as they relate to custody products and services, especially given the bearer nature of digital assets. There is a wide variety of models for maintaining custody of digital assets, each appropriate under different circumstances.

Regulators and lawmakers are increasingly turning their attention to businesses in the digital asset ecosystem, and in some cases have taken action against companies who have acted in contravention of their alleged regulatory obligations. Users, service providers, DACs and other businesses that own or provide services related to digital assets should continue to closely monitor legal and regulatory developments both in the United States and abroad.

[54] *Uniform Commercial Code Amendments (2022)*, <www.uniformlaws.org/viewdocument/final-act-164?CommunityKey=1457c422-ddb7-40b0-8c76-39a1991651ac&tab=librarydocuments>. § § 9-107(A), 9-703, 12-105.

Part 2: Legal Subject Matter Perspectives

Securities Regulation of DeFi

Greg Pesce*

A. General Overview of U.S. Securities Regulation

1. State and Federal Regulation

a. State Regulation and Blue Sky Laws

The offering and sale of securities is heavily regulated at both the federal level and the state level. State securities regulations, often referred to as "blue sky laws," began to be introduced in various states in the early 20th century. Although certain state securities regulators have been active in pursuing actions against various parties involved in crypto-related activity[1] and blue sky laws may generally apply to securities offerings and the licensing of intermediaries such as broker-dealers, agents, salespeople and investment advisers, the scope of state regulation has been significantly reduced since the passing of the National Securities Markets Improvement Act of 1996 and a full discussion of blue sky laws is beyond the scope of this chapter.

b. The Securities Act of 1933

The patchwork of state blue sky laws would prove to be insufficient by the time of the market crash of 1929, and Congress subsequently enacted the first federal securities legislation, the Securities Act of 1933 (the "Securities Act"). The new legislation eschewed the merit-based system used by the blue sky laws in favor of a disclosure-based system, which operates on the basis that the government need not weigh in on the merits of an investment if investors are given the opportunity to make their own informed evaluations through access to full and true disclosure from the issuer, or, to paraphrase Justice Brandeis, that "sunlight is said to be the best disinfectants." To this

---

* Partner, White & Case, Chicago, IL (https://www.whitecase.com/people/gregory-pesce). Lewis Cohen, Partner at Cahill Gordon & Reindel LLP, provided comments on this chapter. Professor Todd Henderson, University of Chicago Law School, reviewed this chapter.

[1] *See, e.g.*, recent enforcement action against BlockFi Lending LLC on February 14, 2022, and Coinbase, Inc. on June 6, 2023.

end, there are two basic objectives underpinning the Securities Act: (i) to ensure that investors receive certain financial and other significant information regarding securities offered for public sale and (ii) to prohibit deceit, misrepresentations and other fraud in the sales of securities. The central thrust of the Securities Act is the regulation of sales of securities from their issuer to purchasers ("primary" sales), and its core is Section 5, which requires registration before the sale of any security unless an exemption is available.

c. The Securities Exchange Act of 1934

The following year, the Securities Exchange Act of 1934 (the "Exchange Act," and together with the Securities Act, the "Securities Acts") broadened federal power over the securities industry by regulating actors, such as brokerage firms, transfer agents, self-regulatory organizations and clearing agencies, in the "secondary" market: sales and purchases between parties other than the issuer of a security. These organizations include the national securities exchanges, of which the two most prominent are the New York Stock Exchange ("NYSE") and the Nasdaq Stock Market ("Nasdaq"). The Exchange Act requires securities listed on such national securities exchanges and certain other securities, such as those traded on over-the-counter networks, to be registered pursuant to its provisions. The issuers of such registered securities are required to satisfy certain periodic and current disclosure requirements. The Exchange Act also created the U.S. Securities and Exchange Commission (the "SEC" or the "Commission"), which took over from the Federal Trade Commission as the regulatory body tasked with administering the securities laws.

2. The Roles of the Commission

The Commission is the principal securities regulator at the federal level and it describes its mission as tripartite: to protect investors, to maintain fair, orderly and efficient markets and to facilitate capital formation.[2] It fulfills this mission through three administrative functions: its legislative or rule-making function, the oversight and regulatory function and its enforcement function. Today, the Commission is one of the most important federal regulatory agencies in the U.S., and it provides oversight of more than $100 trillion annually in securities trading on U.S. equity markets alone.[3] In its rule-making function, the Commission creates rules and regulations under the authority delegated to it by the Securities and Exchange Acts and other legislation. The Commission also articulates its positions in non-binding interpretative releases and Staff Legal Bulletins. Further, it issues so-called "no action letters" when requested by private parties regarding their conduct in particular cases, where the Commission

[2] Securities and Exchange Commission, "Mandate, Mission, Values and Vision," https://www.sec.gov.ph/mandate-mission-values-and-vision/ [perma.cc/ZJ2T-HJ7N].
[3] *Id.*

indicates (without necessarily binding itself to the position) that it will not pursue enforcement action given a set of facts presented to it. In addition, the Commission has several enforcement mechanisms available to it, with remedies that include revocation or suspense of a public company's registration, cease and desist orders, fines and seizure of any ill-gotten gains obtained by wrongdoers.

B. What Constitutes a Security?

1. Statutory Definitions

In order to fall under the jurisdictional purview of the Securities Act and the Exchange Act, a transaction must fit within the definition of a "security." Both the Securities Act[4] and the Exchange Act[5] contain definitions of "securities" that largely overlap and which have been held by the Supreme Court to be "virtually identical."[6] In keeping the with Securities Acts' broad remedial purposes, these definitions are intentionally expansive and have been held to apply to instances related to assets as diverse as orange groves[7] and "self-improvement courses"[8], as well as crypto assets.

---

[4] *See* 15 U.S.C. § 77a (the "Securities Act" defining a "security" [as] 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.)

[5] *See* 15 U.S.C. § 78a (the "Exchange Act" defining a "security" [as] any note, stock, treasury stock, security future, security-based swap, bond, debenture, certificate of interest or participation in any profit-sharing agreement or in any oil, gas, or other mineral royalty or lease, any collateral-trust certificate, preorganization certificate or subscription, transferable share, investment contract, voting-trust certificate, certificate of deposit for a security, 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 instrument commonly known as a "security"; or any certificate of interest or participation in, temporary or interim certificate for, receipt for, or warrant or right to subscribe to or purchase, any of the foregoing; but shall not include currency or any note, draft, bill of exchange, or banker's acceptance which has a maturity at the time of issuance of not exceeding nine months, exclusive of days of grace, or any renewal thereof the maturity of which is likewise limited.).

[6] Tcherepnin v. Knight, 389 U.S. 332, 335 (1967).

[7] *See* SEC v. W. J. Howey Co., 328 U.S. 293 (1946) ("*Howey*").

[8] SEC v. Glenn W. Turner Enterprises, Inc. 474 F. 2d 476 (9th Cir. 1973) ("*Turner*").

2. "Investment Contracts" and crypto assets

a. The *Howey* test

Most instruments commonly described as securities, such as equity instruments like common stock and debt instruments like bonds, are explicitly defined as such in the Securities Act and Exchange Act definitions and treated as such in the market by issuers and purchasers. However, the identification of an unenumerated asset or transaction as a security when this has been in dispute has generally turned on the question of whether such asset or transaction constitutes an "investment contract," an enumerated example of a security in both Securities Acts' definitions. In the landmark Howey decision,9 the Supreme Court held that an investment contract was formed through the sale of tracts of land in orange groves to individuals when combined with service agreements entered into with W.J. Howey Co. that would allow Howey near complete control over the lands to improve upon and share profits with the individuals, and in doing so provided the test for when an asset or transaction will be considered an investment contract. The Supreme Court held that an investment contract "for purposes of the Securities Act means 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, it being immaterial whether the shares in the enterprise are evidenced by formal certificates or by normal interests in the physical assets."[10] In other words *Howey* provides a four-pronged[11] test in which each prong must be satisfied in order for a contract, transaction or scheme to be deemed an "investment contract." The four prongs are:

1. **An investment of money**, which is not limited to cash but has been interpreted widely to include investment of various kinds of assets: as early as 2013, courts have recognized that the exchange of Bitcoin for securities would satisfy this prong.[12]
2. **In a common enterprise**, which focuses on "the extent to which the success of the investor's interest rises and falls with others involved in the enterprise,"[13] or, in other words, that the investment must be into something shared with, and generally controlled by, someone else.

---

[9] See Howey.
[10] *Id.*
[11] The *Howey* test is variously described as having three or four prongs; in the three-pronged formulation prongs three and four presented here are combined into a single prong requiring a reasonable expectation of profits from the efforts of others.
[12] *See, e.g.*, SEC v. Shavers, Fed. Sec. L. Rep. (CCH) 97596 (E.D. Tex. 2013).
[13] Thomas L. Hazen, *The Law of Securities Regulation* 42 (8 ed. 2022).

3. **With a reasonable expectation of profits**, which includes the expectation of capital appreciation of an investor's investment,[14] participation in profits (*i.e.*, dividends)[15] and fixed return instruments.[16]
4. **To be derived from the efforts of others**, which generally requires that the success or failure of the common enterprise is primarily out of the hands of the investor, where "the efforts made by those other than the investor [in managing the enterprise] are the undeniably significant ones."[17]

Since their inception, digital currencies, tokens and other digital and crypto assets have been notoriously difficult to categorize under the *Howey* test. There has also been little in the way of regulatory clarity from the Commission, with the last no-action letter related to digital assets having been issued in November 2020.[18] However, in recent years, the Commission has rather aggressively used the *Howey* test in various enforcement actions against activities related to digital and crypto assets which it views as objectionable, which many commentators, including Commissioner Hester M. Peirce in separate statements from those of the Commission, have derided as "regulation by enforcement."[19] Some common examples of digital assets, organizations and activities are discussed below.

b. Proof-of-Work and Proof-of-Stake

One of the difficulties in the characterization of crypto assets for securities law purposes comes from the way they are created and maintained. Crypto assets are recorded on a "blockchain," which has been described as a "shared, distributed ledger"[20] used for recording transactions. Importantly, no single storage device or server controls the ledger, meaning that a user of a particular blockchain has the same information as any other user, which includes the full history (the "chain") of an asset's every transaction (the "blocks"). Accordingly, each block represents an updating of the state of the overall ledger. To check that the blocks are valid, they are chained together using cryptographic hashes (hence the term "crypto"), which have the property of being easy to decode with the correct cryptographic key but difficult to generate from the underlying encrypted information. These chains are maintained by a widely dispersed

---

[14] *See* United Housing Foundation, Inc. v. Forman, 421 U.S. 837 (1975) ("*Forman*").
[15] *Id.*
[16] *See* SEC v. Edwards, 540 U.S. 389 (2004).
[17] *Turner* at 482 (broadening the prong in *Howey* requiring that the efforts be "solely" of those other than the investor).
[18] Response of the Division of Corporation Finance, IMVU, Inc. (Nov. 17, 2020), https://www.sec.gov/corpfin/imvu-111920-2a1 [https://perma.cc/KW7M-7A3F].
[19] Statement of Commissioner Hester M. Peirce, Great Plains Trust Company (Oct. 2, 2020), https://www.sec.gov/news/public-statement/peirce-dissent-great-plains-2020-10-01 [https://perma.cc/9GBV-T6KZ].
[20] Michael Mendelson, From Initial Coin Offerings to Security Tokens: A U.S. Federal Securities Law Analysis, 22 Stan. Tech. L. Rev. 52, 57 (2019) (citing Manav Gupta, *Blockchain for Dummies* 3 (2017)).

network of computers serving as "nodes" of the blockchain. There are two methods most commonly used to generate "consensus" among blockchain users:

A **proof-of-work ("PoW")** system relies on "miners" for validation. Crypto mining is the process of "solving" a hash by, "in part, guessing a pre-determined number," as the Commission describes it.[21] A solved hash can in turn be used to validate transaction and thus generate new blocks on the chain. This process typically requires the spending of significant amounts of computing power and energy, and miners are incentivized to participate with newly minted crypto assets of that chain, which are typically automatically awarded to successful miners. Bitcoin is perhaps the most well-known crypto asset operating on a proof-of-work system. It is arguable that as the receipt of crypto assets through mining in proof-of-work systems require the expenditure of computational energy by the miner, crypto assets on such systems are less likely to be seen as "derived from the efforts of others" and therefore less likely to be considered securities. Indeed, the Commission has consistently, if only informally, alluded to Bitcoin as not being a security.[22]

A **proof-of-stake ("PoS")** system instead relies on owners of existing crypto assets pledging those assets, known as "staked" crypto, typically for a set period to support the operation of a blockchain. Staked crypto are then algorithmically chosen to be validators for new blocks, with most protocols incentivizing larger stakes by their algorithms. During the staking, the crypto assets will typically be "locked up", not able to be transferred or traded,[23] and there is typically a holding period associated with entering and exiting stake. The practice is meant to incentivize good faith and proper validation, as staked assets may be destroyed permanently, or "slashed", if blocks are not validated appropriately, and validators are rewarded only if new blocks are correctly validated.[24] As the rewards in proof-of-stake systems do not require actually running resource-intensive computations, proof-of-stake systems consume less energy than proof-of-work systems for their validation exercises. The tying of rewards to stakes instead of work also creates the opportunity for multiple parties to pool together their crypto assets and sharing the rewards while delegating the actual validation exercise to a single, specialized entity. Ethereum is the most popular blockchain using a proof-of-stake system, having transitioned from proof-of-work in the so-called "Merge" which completed in late 2022.

---

[21] Complaint at 8, Securities and Exchange Commission v. Payward, Inc. and Payward Ventures, Inc., No. 3:23-Cv-06003 (N.D. Cal., Filed Nov. 20, 2022) ("Kraken Complaint").

[22] *See* Speech by Chair Gary Gentler, Kennedy and Crypto (Sept. 8, 2022) ("By contrast, in the case of a small number of crypto non-security tokens, they might meet some parts of the Howey Test or other tests of a security, but not necessarily all of them, and may not be securities. Bitcoin, the first crypto token, is referred to by some as "digital gold": trading like a precious metal, a speculative, scarce — yet digital — store of value."), https://www.sec.gov/news/speech/gensler-sec-speaks-090822 [https://perma.cc/C96T-4LED].

[23] *See* NOTE: DOES CRYPTOCURRENCY STAKING FALL UNDER SEC JURISDICTION?, 27 Fordham J. Corp. & Fin. L. 521 (lexis.com).

[24] *See* Kraken Complaint at 9.

Not all crypto assets use proof-of-stake or proof-of-work as their consensus mechanisms. For example, XRP, the native token for the Ripple settlement system which will be discussed in further detail below, uses "unique node lists."

c. Non-fungible tokens ("NFTs")

NFTs are digital identifiers, or tokens, recorded on a blockchain that are typically associated with certain unique "metadata" or digital files, including artwork, photography, video and audio, although there is no particular format required for any given asset to be referenced, or, indeed, for any asset to be referenced at all. It can be thought of as a digital marker whose authenticity can be verified through a blockchain. The primary and eponymous distinction NFTs have with cryptocurrencies such as Bitcoin or Ethereum is that an NFT is a digital signature that uniquely identifies it on its blockchain, rendering it "non-fungible" (*i.e.* not able to be treated the same as) any other asset, even those of the same "class" or those originally created by the same entity. Because of their non-fungibility, NFT creators and other market participants often analogize their nature to that of baseball cards or other tangible collectibles that have the potential to appreciate in value.[25] The analogy is particularly appealing given the common conflation of NFTs with the underlying object – usually a piece of digital art – where ownership of the NFT is viewed by market participants as "ownership" of the art, notwithstanding that no copyright or other proprietary interest (*i.e.*, ability to exclude any other person from using or copying the art piece) necessarily passes with an exchange of the token. For the purposes of a *Howey* analysis, the view that NFTs are individualized assets create a challenge for finding of a "common enterprise," making it less likely that any given NFT would be found to be a security.

Dapper Labs – commonality in a controlled system. However, non-fungibility does not necessarily preclude the finding of a common enterprise as a matter of course, which analysis turns heavily on the specific facts of any individual case. In ruling on a motion to dismiss the case of *Friel v. Dapper Labs, Inc.* in February 2023, the District Court for the Southern District of New York held that the plaintiffs in that case had adequately alleged[26] that the defendant Dapper Labs, Inc. had sold securities without a registration statement in contravention of Securities Act Section 5 by offering its NBA Top Shot Moments NFTs ("Moments").[27] In dealing with the issue of a common enterprise, the court noted in particular that the plaintiff "plausibly alleged that

[25] *See*, *e.g.*, Howey Should Think About NFTs and Securities Laws (Sept. 29, 2022) https://www.omm.com/insights/alerts-publications/howey-should-think-about-nfts-and-securities-laws/ [https://perma.cc/YW9J-EBBT].

[26] The procedural posture of the case is important to note briefly. "Adequately alleged" means that, if all facts in the plaintiffs' complaint were true, then the elements of a Section 5 violation would be *prima facie* met. That is, the court has not yet found that there was affirmatively a violation, but simply that as a matter of law, the allegations present in the plaintiff's complaint would be sufficient for such a violation.

[27] *See* Friel v. Dapper Labs, Inc. 2023 U.S. Dist. LEXIS 29176, 62 (S.D.N.Y.).

'Moments' continued value is dependent on the success of Dapper Labs,"[28] as Dapper Labs has complete control over the blockchain on which the Moments exist as well as the proprietary marketplace on which Moments may exclusively be traded. As such, unlike cardboard basketball cards, of which the Moments were claimed by Dapper Labs to be digital analogues, the court observed that "if, hypothetically, Dapper Labs went out of business… the value of all Moments would drop to zero," whereas physical cards may in fact appreciate if their manufacturers fold.[29]

Impact Theory – Founder's Keys and "profits". More recently, in late August 2023 the Commission announced that it had charged Impact Theory, LLC with conducting an unregistered offering of "crypto asset securities" by offering its NFTs, called Founder's Keys, raising "approximately $30 million from hundreds of investors."[30] In particular, the order alleges that Impact Theory had stated, in live speaking events and public statements, that investors could profit from their NFT purchases as investments into the Impact Theory business and that this profit would come from the company's efforts, as the proceeds would be used for "development," "bringing on more team," and "creating more projects."[31] Impact Theory agreed to a cease-and-desist order and paid a total of over $6.1 million in disgorgement, prejudgment interest and a civil penalty without admitting or denying the SEC's charges. The Impact Theory order demonstrates that, just as is the case with orange groves, even if NFTs as an asset class are substantially dissimilar to traditional securities, the application of *Howey* means that particular instances of NFT sales may still be subject to regulatory action where their value and profit expectation are sufficiently tied to a common enterprise whose success depends on the efforts of the promoters, even where any reasonable expectation of profit is limited to capital appreciation devoid of any profit-sharing or fixed return scheme. Here, as Commissioners Hester M. Peirce and Mark T. Uyeda noted in a separate statement, the NFTs "were not shares of a company and did not generate any type of dividend for the purchasers."[32] It is, however, clear that the sale of Founder's Keys were part of capital raising exercise for the expansion of an enterprise similar to initial coin offerings (ICOs), further discussed below, which have been consistently held to be securities offerings. It remains to be seen how future sales of NFTs will react to this new potential landmine.

---

[28] *Id.* at 35.
[29] *Id.*
[30] SEC Charges LA-Based Media and Entertainment Co. Impact Theory for Unregistered Offering of NFTs (Aug. 28, 2023), https://www.sec.gov/news/press-release/2023-163 [https://perma.cc/275G-UGXL].
[31] *See* SEC Charges LA-Based Media and Entertainment Co. Impact Theory for Unregistered Offering of NFTs (Aug. 28, 2023), https://www.sec.gov/news/press-release/2023-163 [https://perma.cc/275G-UGXL].
[32] NFTs & the SEC: Statement on Impact Theory, LLC (Aug. 28, 2023), https://www.sec.gov/news/statement/peirce-uyeda-statement-nft-082823 [https://perma.cc/4SPP-4W5U].

d. Decentralized autonomous organizations and the DAO Report

Inspired by the possibilities for decentralized governance where verification is handled collectively, as in a blockchain, decentralized autonomous organizations, or DAOs, are a form of unincorporated organization built with blockchain technology. As a result, DAOs are generally comprised of large groups of token holders that form for a common purpose, including managing updates to the code underlying an open-source protocol, investing in crypto startups, holding NFTs or generally any other purpose. Once formed, the DAO is supposed to be run by its members without any single person or entity governing or otherwise controlling the decision-making process. Instead, decision-making and voting is done online and often through the use of crypto tokens (usually called "governance tokens"). Governance tokens often enable their holders to cast votes regarding matters of relevance to the DAO. Voting power is based on the number of tokens held. Individuals with a larger number of tokens will have a heavier impact on the voting power for each of the decisions made. The voting system has similarities to typical equity securities but theoretically represents a direct democracy, without a centralized board or management team to provide guidance.

Questions have been raised as to whether the crypto assets representing DAO membership are securities, or if, analogously to most general partnerships, the decentralization of control takes DAO membership outside of this realm. A general partnership interest is typically not an investment contract where each partner takes an active part in managing the business and, as a result, does not rely solely or primarily on the efforts of others. However, a general partnership interest may be considered an investment contract if such partner retains little ability to control the profitability of the investment. The Commission analogized this reasoning in its review (the "DAO Report") of a DAO created by Slock.it UG (known as "The DAO"), a German corporation that it found to be an issuer under U.S. federal securities laws. In its analysis, the Commission applied the *Howey* test and determined that (i) the investors in The DAO invested ether, a cryptocurrency and the native currency of the Ethereum blockchain on which the Slock DAO ran, (ii) the investors invested in a common enterprise through The DAO with the purpose of funding projects that would be proposed by participants, (iii) the investors who purchased the relevant tokens reasonably expected to earn profits since Slock.it and its co-founders informed investors that the DAO was a for-profit entity with the objective to fund projects in exchange for a return on investment and (iv) the investors' profits were to be derived significantly from the managerial efforts of Slock.it, its co-founders and the curators of projects proposed to The DAO by their "whitelisting" certain smart contract business proposals. Further, the Commission found in the DAO Report that the nature of the voting system employed by The DAO naturally diluted and limited the voting rights of the holders of the crypto tokens such that it did not provide them with meaningful control over the enterprise. The Commission noted that token holders' ability to vote for investments was largely a perfunctory one and that holders were widely dispersed and limited in their ability to communicate with one another. Holders voted only on contracts that

were already cleared by the curators, and the method of voting did not provide holders with sufficient information to permit them to make informed voting decisions. In addition, the arrangement of The DAO did not resemble a typical general partnership, which is normally closely held, as there were thousands of individuals participating in The DAO, and certain entities additionally traded the crypto tokens on a separate market. As a result, the Commission found that token holders had no active part in managing the DAO since the sheer number of crypto tokens had diluted any such managerial input to a level comparable to that of a single shareholder in a corporation. Following this analysis, the DAO Report considered The DAO an issuer.[33] Although no remedy was imposed by the Commission in the DAO Report, the report suggested that, had the Commission pursued enforcement, The DAO would otherwise have been required to register the offer and sale of its crypto tokens unless a valid exemption from such registration applied.

e. Crypto lending – *BlockFi* and the *Reves* test

Crypto lending involves a type of secured loan in which an individual's crypto holdings are used in exchange for liquidity from a lender that will be paid off over time. Some crypto exchanges and crypto lending platforms offer this kind of product.[34]

Crypto lending activities may constitute securities under the family resemblance test created by the Supreme Court in *Reves v. Ernst & Young*. The test begins with the rebuttable presumption that every note (an instrument that evidences debt) with a maturity of more than nine months is a security, but such presumption may be rebutted

---

[33] 15 U.S.C. § 78a (the "Exchange Act" defining an "issuer" [as] every person who issues or proposes to issue any security; except that with respect to certificates of deposit, voting-trust certificates, or collateral-trust certificates, or with respect to certificates of interest or shares in an unincorporated investment trust not having a board of directors (or persons performing similar functions) or of the fixed, restricted management, or unit type, the term "issuer" means the person or persons performing the acts and assuming the duties of depositor or manager pursuant to the provisions of the trust or other agreement or instrument under which such securities are issued; except that in the case of an unincorporated association which provides by its articles for limited liability of any or all of its members, or in the case of a trust, committee, or other legal entity, the trustees or members thereof shall not be individually liable as issuers of any security issued by the association, trust, committee, or other legal entity; except that with respect to equipment-trust certificates or like securities, the term "issuer" means the person by whom the equipment or property is or is to be used; and except that with respect to fractional undivided interests in oil, gas, or other mineral rights, the term "issuer" means the owner of any such right or of any interest in such right (whether whole or fractional) who creates fractional interests therein for the purpose of public offering.).

[34] In the Matter of Blockfi Lending LLC, ORDER INSTITUTING CEASE-AND-DESIST PROCEEDINGS PURSUANT TO SECTION 8A OF THE SECURITIES ACT OF 1933 AND SECTION 9(f) OF THE INVESTMENT COMPANY ACT OF 1940, MAKING FINDINGS, AND IMPOSING A CEASE-AND-DESIST ORDER, File No. 3-20758 (Feb. 14, 2022), https://www.sec.gov/files/litigation/admin/2022/33-11029.pdf. ("BlockFi Lending LLC Cease-and-Desist").

if the note bears a resemblance to one of any enumerated categories on a judicially developed list of exceptions. These exceptions are[35]:

1. A note delivered in consumer financing;
2. A note secured by a mortgage on a home;
3. A note secured by a lien on a small business or some of its assets;
4. A note relating to a "character" loan to a bank customer;
5. A note which formalizes an open-account indebtedness incurred in the ordinary course of business;
6. Short-term notes secured by an assignment of accounts receivables;
7. Notes given in connection with loans by a commercial bank to a business for current operations.

Crypto lending first came under the Commission's scrutiny in 2022, when the Commission announced a settlement with BlockFi Lending LLC. The settlement was made with respect to BlockFi's alleged failure to register the offer and sale of its retail crypto lending product. BlockFi, a financial services company, offered and sold BlockFi Interests Accounts ("BIAs") to investors, by which the investors would lend their crypto assets to BlockFi in exchange for BlockFi's promise to provide a variable monthly interest payment. These interest payments were made in a variety of ways including loans of crypto assets, lending U.S. dollars to retail investors and investing in equities. The Commission found that based on the facts and circumstances, the BIAs were securities under the *Reves* test because they were notes. The presumption that such notes were securities could not be rebutted, as there was no family resemblance to any one of the enumerated categories.[36]

f. Crypto Staking "as a service" - *Kraken*

As discussed above, on proof-of-stake systems it is possible for crypto stakers to "pool" their assets together. The benefit of this is that larger stakes are typically preferred as validators by system algorithms and thus are more likely to receive the corresponding crypto rewards. As a result, certain cryptocurrency exchanges, such as the Kraken Crypto Exchange, began offering "staking as a service" programs, whereby investors would pool their stakes to be managed by Kraken. On February 9, 2023, the Commission announced that it had instituted and settled an enforcement action against Kraken in which the Commission alleged the staking service it provided and marketed was an unregistered public offering of securities. The Commission alleged that the Kraken staking service was an investment contract security since the investors made (i) an investment of money by committing their assets to the mandatory lock-up with the

[35] Reves v. Ernst & Young, 494 U.S. 56 (1990).
[36] BlockFi Lending LLC Cease-and-Desist.

intention of securing rewards from the lock-up of their crypto assets, (ii) the investment was made to the common enterprise of Kraken, which pooled the assets from multiple investors, (iii) the investors had a reasonable expectation of profits from Kraken's efforts through its advertising of returns through the staking service and (iv) the investors relied on Kraken's equipment, expertise and resources to compete in the staking market and provide adequate staking services. The Kraken settlement required the company to discontinue its staking program and pay $30 million in disgorgement, prejudgment interest and civil penalties.

The Commission's handling of the Kraken enforcement action has sparked controversy. Commissioner Peirce dissented from the Commission's decision. She noted that the Commission did not think through staking programs individually, despite the fact that each may exhibit unique characteristics. Further, she noted that rather than issuing guidance, the Commission chose to use enforcement action to shut down a program that was serving investors well and such actions being used to tell the law in an emerging industry is an inefficient and unfair way to regulate.[37] Although the enforcement action has led to uncertainty in the market, staking as a service activity has continued, learning from the Kraken action and adjusting their approach. One example is Kiln, a company created to provide staking services for crypto custodians. The company has stated that they believe they provide a framework to allow crypto institutions and their customers to stake that is SEC-compliant. Contrary to Kraken, Kiln notes that they never possess custody of the crypto assets and that there are no lending or early liquidity options in their service. The Commission has not yet commented on Kiln's model.

3. Characterizing Offerings of Crypto Assets

As a consequence of the focus in the Securities Act on transactions, in some cases judgment on whether a crypto asset has been involved in a security will depend on *how* the sale or transfer of the crypto asset has been effected and what was communicated to the purchaser in connection with the sale. The *SEC v. Ripple Labs, Inc*. case from July of 2023 demonstrates this, as certain sales of its token, such as XRP, were found to be unlawful sales of securities, while certain others were not. In *Ripple*, the Commission brought an action against Ripple Labs, Inc. and two of its senior leaders, Bradley Garlinghouse and Christian A. Larsen. The action alleged that the defendants engaged in the unlawful offer and sale of securities in violation of Section 5 of the Securities Act. Ripple was founded in 2012 by Larsen and another co-founder and at its core is the XRP ledger, a software code that "operate[d] as a peer-to-peer database, spread across a network of computers, that records data respecting transactions, among other things." In 2013, Ripple began distributing XRP with public statements that, in the eyes of the

[37] See, *e.g.*, Dissent of Commissioner Hester Pierce, available at https://www.sec.gov/news/statement/peirce-statement-kraken-020923.

Commission, gave investors reason to believe that Ripple's efforts would produce profits for holders of XRP. The Commission alleged that Ripple engaged in three categories of unregistered securities offers and sales: (i) "institutional sales" negotiated directly by Ripple Labs with institutional buyers, for which it received $728 million, (ii) so-called "programmatic sales" on a blind-bid basis on digital asset exchanges, for which it received $757 million; and (iii) other distributions under written contracts for which it recorded $609 million in "consideration other than cash." To determine whether a registration statement was required, the Southern District Court of New York analyzed each of these three types of XRP transactions under the *Howey* test. Importantly, the court noted that "XRP, as a digital token, is not in and of itself a "contract, transaction[,] or scheme" that embodies the Howey requirements of an investment contract" and that the totality of circumstances around each of the kinds of transactions would need to be analyzed.[38]

With respect to institutional sales, the court held that the sale of XRP was in violation of Section 5 of the Securities Act since investors made (i) a payment of money for XRP, (ii) there was a common enterprise, in which an investor's assets were pooled and the fortunes of each investor were tied to the fortunes of other investors and (iii) based on the materials provided by Ripple to institutional buyers to induce their purchases, reasonable investors would have made their purchases of XRP with the expectation that they would derive profits from Ripple's efforts. Ripple made several marketing statements directly to the institutional investors that tied future price increases in XRP's value to Ripple's efforts to increase the value of the XRP network and the XRP token.

The court applied a similar analysis for programmatic sales. In this case, the court instead held that programmatic sales did not violate Section 5 of the Securities Act since it found that the Commission had failed to establish the presence of the third prong and fourth prongs of *Howey*. The court noted that the nature of these sales was different from institutional sales due to the indirect purchase via digital asset exchanges where 99% of the trading volume was unrelated to any sales by Ripple Labs. The programmatic sales were blind-bid transactions, which means that purchasers could not have known if their payments of money went to Ripple or any other seller of XRP. As a result, the programmatic buyers could not reasonably expect that Ripple would use the capital it received from its sale to improve its enterprise and increase the price of XRP. The court noted that some programmatic purchasers may have bought XRP with an expectation of profits, but they did not reasonably derive that expectation from Ripple's efforts since Ripple made no promises or offers to such purchasers.

The court also analyzed other distributions under the *Howey* test and held that there were no other violations of Section 5 of the Securities Act since distributions to employees as compensation and to third parties developing new applications for XRP

[38] SEC v. Ripple Labs, Inc., 2023 U.S. Dist. LEXIS 120486, 24 (S.D.N.Y.) ("Ripple").

did not satisfy the first prong of an investment of money. The recipients of XRP in these distributions did not provide any tangible or definable consideration.

It remains uncertain whether other courts will adopt the reasoning in *Ripple*. Shortly after the *Ripple* decision, in the context of a motion to dismiss by the defendants the senior judge in the Southern District of New York court expressly refused to adopt the *Ripple* court's interpretation of the *Howey* test. In *SEC v. Terraform Labs Pte. Ltd.*,[39] Terraform, a Singapore based company, developed the Terraform blockchain and sold the "Terra/UST" stablecoin (a cryptocurrency that is intended to be pegged to a stable asset, such as a fiat currency or commodity) and the "LUNA" native token. Unlike as was the case in *Ripple* where no investor loss or fraud was alleged, in the *Terraform Labs* case, investors suffered billions of dollars of losses and there were multiple allegations of fraud on the part of the promoters by the Commission. Terraform made claims that the stablecoin UST, was algorithmically backed by its sister token LUNA, which enabled UST to have a fixed price of exactly $1.00. However, UST became unstable and started losing value, causing investors to worry that the coin would not stabilize on its own which prompted Terraform to enter into an agreement with a third-party trading firm based in the U.S. to buy a large number of UST coins to restore the $1.00 value. Terraform concealed the true nature of the issue and claimed that the UST stablecoin had returned to value on its own. As a result, investors re-invested billions in Terraform. Exactly one year later, the market crashed with LUNA coins being sold or converted at a high rate causing both coins to plummet to under a penny and wiping out over $40 billion of total market value for investors.

The court applied the *Howey* test to Terraform and found that, based on the Commission's pleadings, there was at least a plausible claim that each crypto asset qualified as a security. However, in contrast to *Ripple*, the court declined to draw a distinction between the crypto assets based on their manner of sale and rejected the *Ripple* approach that coins sold directly to institutional investors would be considered securities and require registration or an exemption that those sold through the secondary market transactions to retail investors are not. The court in *Terraform* noted that *Howey* made no such distinction and that if the allegations are true, Terraform clearly "embarked on a public campaign to encourage *both* retail and institutional investors to buy their crypto-assets by touting the profitability of the crypto-assets and the managerial and technical skills that would allow the defendants to maximize returns on the investors' coins." However, in doing so *Terraform* appears to mischaracterize the approach taken in *Ripple*, as the *Ripple* court simply applies the *Howey* test to each of the specific transactions identified by the Commission. This approach of analyzing each transaction separately was subsequently validated in a civil suit dismissed by another Southern District of New York judge.[40]

The Commission has also applied enforcement actions in other aspects of crypto offerings including for the failure of an exchange which hosts offerings to register as a

[39] SEC v. Terraform Labs Pte. Ltd., 2023 U.S. Dist. LEXIS 132046. (S.D.N.Y.).
[40] Risley v. Universal Navigation Inc., 2023 U.S. Dist. LEXIS 152946 (S.D.N.Y.).

national securities exchange. On April 17, 2023, the Commission charged crypto asset trading platform Bittrex, Inc. and its former CEO, William Shihara, for operating as an unregistered national securities exchange, broker, and clearing agency. Bittrex was in the process of winding down its U.S. business at the time. In the complaint, the Commission alleged that Bittrex earned at least $1.3 billion from providing services typically connected to brokers, exchanges and clearing agencies for securities transactions. The alleged services include soliciting potential investors, handling customer funds and assets and charging fees for such services, holding customers' assets in Bittrex controlled wallets and settling customer transactions. In addition, the Commission alleged that Bittrex operated as an unregistered securities exchange since it provided a marketplace that brought together orders of multiple buyers and sellers of crypto assets and matched and executed those orders. The Commission also alleged that Bittrex employed a coordinated campaign with prospective issuers to delete from public channels "investment related terms" that could raise questions about whether the crypto assets being offered could be considered securities. The Commission characterized such actions as "cosmetic alterations" that "did nothing to change the underlying realities of the offerings and Bittrex's conduct."[41] On August 10, 2023, Bittrex and the Commission agreed to settle the charges. The settlement, among other things, requires the defendants to pay a disgorgement of $14.4 million, prejudgment interest of $4 million and a civil penalty of $5.6 million.[42]

C. Transfer Mechanics

1. Certificated and Uncertificated Securities

The mechanics relating to the transfer of ownership, or "negotiation", of securities are governed under Article 8 of the Uniform Commercial Code ("UCC"). Securities may be certificated or uncertificated.

A certificated security is defined in Section 8-102 as "an instrument issued in bearer or registered form that is of a type commonly dealt in on securities exchanges or markets or commonly recognized as a medium for investment." A certificated security is in registered form where the certificate "specifies a person entitled to the security or the rights it represents."[43] A certificated security is in "bearer form" when it is "payable to bearer according to its terms and not by reason of any indorsement." The "bearer" is

---

[41] *See* SEC Charges Crypto Asset Trading Platform Bittrex and its Former CEO for Operating an Unregistered Exchange, Broker, and Clearing Agency (April 17, 2023) https://www.sec.gov/news/press-release/2023-78 [https://perma.cc/Y8MY-NG6K].

[42] See Crypto Asset Trading Platform Bittrex and Former CEO to Settle SEC Charges for Operating an Unregistered Exchange, Broker, and Clearing Agency (Aug. 10, 2023), https://www.sec.gov/news/press-release/2023-150 [https://perma.cc/8UGE-RRZG].

[43] U.C.C. § 8-102. Definitions.

the person who holds the certificate, irrespective of competing claims to the security.[44] While historically, corporate debt issuances have sometimes been in certificated bearer notes, recent trends have moved away from the corporate issuance of certificated debt securities. Further, equity has generally not been issued in certificated form in the United States, with one important reason being that both the NYSE and Nasdaq require all listed securities to be in book entry.

An uncertificated security is not represented by a written instrument and the transfer of the security is registered upon books maintained for that purpose by or on behalf of the issuer. These uncertificated securities are commonly referred to as "book entry" securities. Listed companies' securities registers are maintained by a transfer agent and are held through the Depository Trust Company, a central securities depository that manages book-entry securities.

2. UCC Article 8 and Proposed UCC Article 12

Currently, the most common means evidencing a transfer in crypto assets is through the "Financial Asset" structure of Part 5 of UCC Article 8. Under the financial asset structure, a person acquires a financial asset, other than a security, if the person acquires a security entitlement to the financial asset.[45] Any property held by a securities intermediary for another person in a securities account may be considered a financial asset if expressly agreed upon, including crypto assets. An express agreement between the parties defines who may serve as a securities intermediary and what may be considered a securities account. Once the crypto asset is deposited into the securities account, the owner becomes holder of the securities entitlement. Through this structure, a security interest in the crypto assets is perfected when the party obtains control of the securities entitlement. Control of a securities entitlement means (i) the purchaser becomes the entitlement holder; or (ii) the securities intermediary has agreed that it will comply with entitlement orders originated by the purchaser without further consent by the entitlement holder; or (iii) another person has control of the security entitlement on behalf of the purchaser or, having previously acquired control of the security entitlement, acknowledges that it has control on behalf of the purchaser.[46] Once control is established, the entitlement holder may transfer control of the securities entitlement and the crypto assets to a transferee as part of a sale.

In light of the rapid rise of crypto assets, the Uniform Law Commission and the American Law Institute have proposed new amendments to the UCC. The new amendments would provide for an entirely new article of the UCC. The proposed UCC Article 12 creates a class of digital assets defined as "controllable electronic records"

---

[44] *Id.*

[45] See U.C.C. § 8-104. Acquisition of Security or Financial Asset or Interest Therein Definitions.

[46] U.C.C. § 8-106. Control.

("CERs").[47] A CER is a "record stored in an electronic medium that is susceptible to 'control.'" The purpose of UCC Article 12 is to provide legal certainty on the applicable of certain aspects of commercial law to crypto assets since crypto assets did not fit squarely into UCC Article 9's definition of general intangibles. Under the proposed new Article 12, control is defined as when a holder is able to derive "substantially all the benefit" from the CER and has "exclusive power" to "prevent others from availing themselves of substantially all the benefit" from the CER. In addition, the CER must allow the holder to be able readily to identify the CER in any way, including by cryptographic key, as having these exclusive powers. Under this proposed form of "control," a holder is considered a "qualifying purchaser" with super-priority status over any other security interest in the crypto asset, even prior perfected UCC filers. This allows a CER to be transferred in such a way that cuts off competing security interest claims.

D. Securities Offerings

1. Trigger Regulation: "Sales" and "Offers"

Under Section 5 of the Securities Act, a registration statement is required for the offer and sale of any securities, unless an exemption is available. A "registration statement" is a document that contains certain disclosure about the company, the securities and the offering as prescribed by the Commission. The Securities Act defines the term "sale or sell" broadly to include "every contract of sale or disposition of a security or interest in a security for value." Such transactions include exchanges of securities for cash or other securities and written commitments to deliver shares of stock. Generally, a sale occurs at the moment the parties become obligated to perform the securities transaction. This means that a contract may be a sale even if it is never fully performed. The term "offer" is even broader and includes every attempt to offer or dispose of or solicitation of an offer to buy a security or interest in a security, for value.[48] An offer may be any form of communication that indicates an intent by the issuer to procure orders for a security, arouse public interest in or "condition the public mind" about a security. When a security is involved, these types of communications will trigger an obligation by the issuer to file a registration statement for the offering and sale of the securities.

The process of preparing a registration statement is lengthy and costly due to the substantial and stringent disclosure and formal requirements and because in most cases

[47] See Steven R Aquino, Crypto, Part III: Securing Interests in Digital Assets—The Proposed UCC Article 12, American Bar Association (May 23, 2023), https://www.americanbar.org/groups/litigation/resources/newsletters/corporate-counsel/crypto-part-3-securing-interests-digital-assets-the-proposed-ucc-article-12/.

[48] See 15 U.S.C.A. § 77b. Definitions; promotion of efficiency, competition, and capital formation.

the Commission will require significant time to review the statement before it may be declared effective. Until the registration statement is declared effective the issuer may not sell the securities covered by it.[49] The Commission has established numerous regulations to prescribe the information required in a registration statement, including Regulation S-K for their substantive disclosure requirements and Regulation S-X for applicable financial statements. The Commission has also prepared extensive guidance in an effort to promote uniformity and to ensure material information is provided to potential purchasers. While there are various forms of registration statements, the most commonly used are Forms S-1, S-3 and S-4. Form S-1 is the most widely used registration statement form, requiring "long-form" disclosure and usually used for Initial Public Offerings (IPOs). Form S-3 is a "short-form" registration statement available for issuers that already have reporting history for offerings after an IPO. Form S-4 is used in certain circumstances where securities are exchanged for other securities, most commonly in a public company merger. Foreign issuers have a parallel registration statement forms available in Form F-1, F-3 and F-4, which have reduced disclosure requirements compared to their domestic counterparts but generally also require compliance with the rules in an issuer's home country.

Further, under the Exchange Act, listed issuers must file reports on a quarterly and annual basis, which disclosure must include information regarding the issuer's business, operations and financial results. Domestic reporting companies are expected to file an annual report on Form 10-K, filed after the end of the issuer's fiscal year; quarterly reports on Form 10-Q, filed after the end of each of the issuer's first three quarters; and current reports on Form 8-K for certain specified events or corporate changes that trigger such disclosure. Compliance with such ongoing disclosure requirements is another significant cost for public reporting companies.

2. Initial Coin Offerings

An Initial Coin Offering ("ICO") is a fundraising mechanism for startups and businesses involved in the cryptocurrency and blockchain space. An ICO can be viewed as the crypto asset parallel to an (IPO) of securities.

ICOs raise a number of potential problems with the established rules of securities offerings. For example, although ICOs most likely constitute securities transactions, the crypto asset sold may not itself be a security, thus leaving open questions of the applicability of the securities laws to secondary transactions in crypto assets. To date, all litigated SEC enforcement actions related to ICOs have involved allegations of Section 5 violations as a result of unregistered fundraising transactions which the Commission considered to fall within the *Howey* test as "contracts, transactions or schemes" and the status of a crypto asset itself as a security regardless of the transaction in which it is sold has not been at issue and has not been addressed by the holding of any court.

[49] See 17 CFR § 210.7-02. General requirement.

Due to a lack of regulatory oversight and frequent overheated interest on the part of purchasers eager to catch the "next big thing," many fundraising sales of crypto assets through ICOs have involved misleading, if not outright fraudulent, inducements to purchase, with many crypto assets losing all or substantially all of their value within a short period of the ICO. In response, other techniques were developed, including Initial Exchange Offerings ("IEOs") and Initial Decentralized Exchange Offering ("IDOs"). IEOs involve a centralized crypto exchange in which the initial listing would be placed; in theory, the exchange will have vetted the project and ensured its legitimacy (although, more frequently, the exchange extracts a fee for listing and provides little or no quality control).[50] IDOs involve a decentralized crypto asset exchange (known as a DEX) in which the relevant crypto asset is made available in "liquidity pool" and available to be purchased by anyone accessing the DEX platform, with the price set by supply and demand. Nevertheless, the issues associated with ICOs remain present in IEOs and IDOs. Regardless of the means of the initial offering of the crypto currency, the Commission and the courts considering these transactions to date have generally agreed that crypto asset fundraising transactions made available to the general public in the U.S., whether through ICOs, IEOs or IDOs, are subject to the registration and prospectus delivery requirements required under federal securities law.[51]

INX Limited provides an example of a crypto asset security initial coin offering being registered. INX initially filed their public offering on August 19, 2019, for 130,000,000 INX Tokens.

3. Section 4(a)(2) Private Placements

Securities issued in an exempt offering may not be immediately resold without an available exemption for resale or subsequent registration. These securities are generally referred to as "restricted." One of the most common exemptions is found Section 4(a)(2), a private placement exemption. In order to rely on the Section 4(a)(2) exemption, the investors in the private placement must (i) either have sufficient knowledge and experience in finance and business matters to be a sophisticated investors or have the ability to bear the investment's economic risk, (ii) have access to the type of information that normally is provided in a registration statement and (iii) agree not to resell or distribute the private placement securities to the public. Some factors that go into determining whether an offering falls under the exemption with Section 4(a)(2) is the number of investors, the presence or absence of a general solicitation, the information provided and investor intent. Generally, having fewer investors in the private placement evidences a lack of public offering. Further, unless the requirements of the SEC's Rule 506(c) (discussed below) are met, a general solicitation or public advertising of the private placement would likely cause the transaction to be considered a public

[50] See Gemini, IEOs and IDOs: An Evolution in Crypto Fundraising (Oct. 21, 2021), https://www.gemini.com/cryptopedia/ieo-crypto-ido-crypto-initial-exchange-offering.

[51] See Bromberg & Lowenfels on Securities Fraud, § 23:1. Introduction, at 7 (2d ed.).

offering. Finally, any intent of the investors to quickly resell the privately placed securities would also increase the chance of the transaction being considered a public offering.[52]

4. Regulation D

Regulation D provides additional separate safe harbor exemptions under Rules 506(b) and 506(c). Through Rule 506(b), the Commission provided objective standards that issuers could rely on to meet the requirements of the Section 4(a)(2) exemption. Rule 506(b) allows for issuers to conduct an offering that may raise an unlimited amount of money and sell securities to an unlimited number of accredited investors, so long as: (i) no general solicitation or advertising is made to market the securities and (ii) the securities may not be sold to more than 35 non-accredited investors. If any non-accredited investors are participating in the offering, the issuer must provide disclosure documents consistent with Regulation A offerings, financial statement information specified in Rule 506 and be available to answer questions from the non-accredited investors. Rule 506(c) provides a safe harbor for issuers who would like to participate in a broad solicitation and general advertisement of the offering but requires that: all purchasers in the offering are accredited investors, the issuer took reasonable steps to verify the purchasers' accredited investor status and reasonably believes that they are accredited investors. Similar to Rule 506(b), there is no set limit on the number of accredited investors or the amount that may be raised.[53]

5. Regulation A

Another exemption potentially available is Regulation A. Under the initial rules, Regulation A permitted unregistered public offerings of up to $5 million of securities in any 12-month period. However, the combination of a disclosure document that required SEC review and the requirement to have to separate state law qualifications made the initial provisions of Regulation A burdensome and rarely used by issuers. On June 19, 2015, the Commission adopted final rules to update the exemption to help facilitate access to capital for smaller companies and provide more investment choices for investors. The revised Regulation A is often informally called "Regulation A+." Under the updated rules, private companies can offer up to $75 million of securities in a 12-month period. These updated rules offer two tiers of offerings:

1. Tier 1 permits offerings of up to $20 million within a 12-month period that may not include more than $6 million on behalf of affiliated selling security holders.

[52] 17 C.F.R. § 230.506(b).
[53] 17 C.F.R. § 230.500. Use of Regulation D.

2. Tier 2 permits offerings of up to $75 million within a 12-month period that may not include more than $22.5 million on behalf of affiliated selling security holders.

For the initial Regulation A offering and any subsequent Regulation A offerings in the 12 months following the initial offering, selling security holders may not sell more than 30% of the total offering. After the first year of the initial Regulation A offering, non-affiliate selling security holders may sell up to 100% of the offering, but affiliate selling security holders are still limited to 30% of the aggregate offering. The new rules allow issuers to advertise the offering, and anyone can invest, subject to the certain dollar amount limitations for non-accredited investors. Like the prior rules, a Regulation A offering requires (i) an offering statement that is subject to SEC review, (ii) audited financial statements and (iii) semi-annual reporting obligations for the issuer if the offering is greater than $20 million.54

Crypto issuers that have used the Regulation A exemption include Blockstack Token, LLC and Open Props Inc. In 2019, Blockstack Token raised more than $15 million in a token sale qualified under Regulation A. The offering raised $15.5 million through the sale of 74.3 million Stacks tokens. The sale was divided into two lots. The first lot sold 36.4 million tokens directly and raised approximately $10.9 million. The second lot was sold through a voucher program and added an additional $4.6 million55. Open Props received Commission qualification shortly afterward for a Regulation A offering. In 2021, Open Props announced that by the end of the year they would end the program and discontinue issuing new Props tokens under Regulation A. Among the issues cited by Open Props was the regulatory constraints of Regulation A. The company noted that:

"[t]he Reg A+ continuous offering environment in which we operate requires us to make public filings and often get prior regulatory approval for product changes. As a result, we are unable to follow anything remotely like proper product development of "launch, measure, iterate" and struggle to launch new key functionalities we develop (like staking or per-app tokens)."56

Similarly, Blockstack reportedly spent approximately $1.5 million on legal fees and the Commission's review process of the Regulation A offering took around 10 months from when Blockstack submitted its confidential draft filing.57 This timing is significantly longer than the typical filing process for a Regulation A offering, which is usually estimated to take approximately four to six months.

---

[54] 17 C.F.R. § 230.251. Scope of exemption.

[55] See Paul Vigna, SEC Clears Blockstack to Hold First Regulated Token Offering, The Wall Street Journal (July 10, 2019), https://www.wsj.com/articles/sec-clears-blockstack-to-hold-first-regulated-token-offering-11562794848.

[56] Business Wire, Props Launches the First SEC-Approved Crypto Token for Consumers (July 11, 2019), https://www.businesswire.com/news/home/20190711005651/en/Props-Launches-the-First-SEC-Approved-Crypto-Token-for-Consumers.

[57] See JR Lanis, Fiammetta S. Piazza, Sec Qualifies First Regulation A+ Offerings of Blockchain-Native Digital Assets: Blockstack and Younow, Orange County Law., at 48 (October 2019).

6. Regulation Crowdfunding

Regulation Crowdfunding, or Regulation CF, provides another exemption to the registration requirements under the federal laws. For an issuer to be eligible to offer and sell securities through crowdfunding they must: (i) require all transactions under Regulation CF to take place online through a Commission registered broker-dealer or funding portal, (ii) only issue a maximum aggregate amount of $5 million through crowdfunding offerings in a 12-month period, (iii) limit the amount individual non-accredited investors can invest across all crowdfunding offerings in a 12-month period based on the non-accredited investors income or net worth and (iv) require disclosure of information in filings with the Commission and to investors and the intermediary facilitating the offering. In addition, any type of U.S. entity can utilize Regulation CF and may sell securities in all 50 states. Like most disclosure required in capital raises, the issuer must provide disclosure that includes financials, descriptions of officers, directors, significant stakeholders, use of proceeds, and material risks. Issuers are limited in the information they may provide as a general solicitation or advertisement done outside of the portal.[58]

7. No-Action Letters

Issuers who are unsure if their particular product, service or action would potentially violate federal securities law may request a "no-action" letter from the staff at the SEC. Issuer requests typically include lengthy legal analysis in support of an issuer's position that the Commission take no enforcement action against specified issuer actions. If the Commission agrees, it will issue a no-action letter tailored to the circumstances specified in the request confirming that it will not pursue enforcement action. In the proposed offer by TurnKey Jet, Inc. to sell blockchain-based digital assets in the form of tokenized "jet cards," the Commission issued a no-action letter which agreed with TurnKey Jet's analysis, specifically noting that: (i) the tokens will be immediately useable for their intended functionality (purchasing air charter services), (ii) the tokens were marketed in a manner that emphasized their intended functionality as opposed for their potential increase in the market value of the token, (iii) TurnKey Jet is not using any of the funds to develop the platform or app, and (iv) TurnKey Jet will sell the tokens at a price of one USD per token throughout the life of the program (effectively eliminating a secondary market to increase the value of the token) and each token represents the obligation to supply air charter services at a value of one USD per token.[59] Similar reasons were cited in additional no-action letters sent shortly after the TurnKey Jet, Inc. letter. In 2019, the Commission did not recommend an enforcement

[58] See 17 C.F.R. § 240.12g–6. Exemption for securities issued pursuant to section 4(a)(6) of the Securities Act of 1933 or Regulation Crowdfunding.

[59] Response of the Division of Corporation Finance, TurnKey Jet, Inc. (Apr. 3, 2019), https://www.sec.gov/divisions/corpfin/cf-noaction/2019/turnkey-jet-040219-2a1.htm.

action against Pocketful of Quarters, Inc, which intended to issue "Quarters" through blockchain technology to consolidate various video-game currencies from participating video games to a singular wallet. Applying similar analysis, the Commission noted that (i) the quarters would be immediately useable for their intended purposes, (ii) Pocketful of Quarters marketed and sold the Quarters to gamers solely for consumptive use, (iii) no funds from Quarters sales would be used to build the platform and (iv) the Quarters were sold continuously in unlimited quantities and at a fixed retail price, which eliminated the secondary market.[60]

8. The Problem of "Touting" in Crypto

On November 1, 2017, the Commission recognized the growing use of celebrities and other influencers through social media platforms to endorse investments in the cryptocurrency space and issued a "Statement Urging Caution around Celebrity Backed ICOs." The statement reiterated the long-standing tenet in federal securities law that endorsements of securities may be unlawful if the influencer does not disclose the nature, source and amount of any compensation paid, directly or indirectly, by the company in exchange for the endorsement.[61] One of the more notable cases stemmed from the Ethermax enforcement actions. Ethermax had paid reality TV star Kim Kardashian approximately $250,000 in exchange for promotion of the crypto tokens to her 225 million Instagram followers. The resulting post caused the tokens to balloon in price, but their value quickly crashed. The Commission found Kardashian in violation of Section 17(b) of the Securities Act and ordered her to pay a fine of $1,000,000 and a disgorgement of the $250,000.[62] The Commission also prosecuted Paul Pierce, former NBA star, for his endorsement of Ethermax. Pierce sent several tweets to his more than 4 million followers, promoting Ethermax in exchange for approximately 244,000 tokens. Pierce failed to state the required disclosures and was found in violation of Section 17(b) of the Securities Act. Further, the Commission alleged that Pierce negligently misrepresented the amount of compensation he received from Ethermax by posting that he received a quantity of tokens that was valued at more than $2.5 million. Pierce agreed to pay $1.4 million in disgorgement and penalties. Both Kardashian and Pierce were also prohibited from promoting crypto asset securities for three years.[63] It is clear through both examples and continuing enforcement actions, such as in its March 22,

---

[60] Response of the Division of Corporation Finance, Pocketful of Quarters, Inc. (July 25, 2019), https://www.sec.gov/corpfin/pocketful-quarters-inc-072519-2a1.

[61] SEC Division of Enforcement and SEC Office of Compliance Inspections and Examinations, SEC Statement Urging Caution Around Celebrity Backed ICOs (Nov. 1, 2017), https://www.sec.gov/news/public-statement/statement-potentially-unlawful-promotion-icos.

[62] SEC Charges Kim Kardashian for Unlawfully Touting Crypto Security (Oct. 3, 2022), https://www.sec.gov/news/press-release/2022-183.

[63] SEC Charges NBA Hall of Famer Paul Pierce for Unlawfully Touting and Making Misleading Statements about Crypto Security (Feb. 17, 2023), https://www.sec.gov/news/press-release/2023-34.

2023 charges against eight celebrities for touting Tronix and BitTorrent,[64] that the Commission is aggressively looking to enforce its anti-touting policy in the crypto currency space.

9. Regulation S; Limits of SEC Jurisdiction

Regulation S provides an SEC compliant exclusion from the registration requirements of the Securities Act for offers made outside the United States to non-U.S. persons. The safe harbor is available if: (i) the securities are sold in an offshore transaction and (ii) there are no directed selling efforts in the United States. Further, offers and sales of are subject to additional restrictions based on their categorization under Rule 903(b). "Category 1" offerings are those in which the securities are the least likely to flow back into the United States hence, the only restrictions to Category 1 is that it must be an "offshore transaction" and that there be no "directed selling efforts" in the United States. "Category 2" and "Category 3" offerings become subject to an increasing number of restrictions for the duration of the applicable "distribution compliance period" due to the likelihood that the securities may flow back into the United States. A "distribution compliance period" typically ranges from 40 days to six months for reporting issuers or one year for non-reporting issuers. The period begins shortly following the offering when any offers or sales of Category 2 or 3 securities must be made in compliance with the requirements of Regulation S to prevent the flow back of the offered securities into the United States. To qualify as an offshore transaction the offer or sale must be made to a person outside the United States in which either (i) at the time the buy order is originated, the buyer is outside the United States or the seller reasonably believes so, or (ii) the transaction is executed on a foreign securities exchange located outside the United States (for the issuer safe harbor) or through the facilities of a designated offshore securities market (for the resale safe harbor). Generally, a directed selling effort exists where there is any activity that would have or could reasonably be expected to have an effect of conditioning the market in the United States in connection with the securities offered in reliance under Regulation S.[65]

In 2010, the Supreme Court decision in *Morrison v. National Australia Bank Ltd*. limited the extraterritorial application of federal securities laws, notwithstanding some articulable connection to the United States.[66] In *Morrison*, the Australian plaintiffs asserted fraud under American federal securities laws since their stock declined in an Australian bank due to statements made by the bank's U.S. subsidiary. The Court held that such connection to the U.S. was too remote and tenuous for American securities law to apply. As a result, the Court found that when Section 10(b) is properly applied, it allows for only domestic claims brought by plaintiffs that (i) "transact in securities

[64] See SEC Charges Crypto Entrepreneur Justin Sun and His Companies for Fraud and Other Securities Law Violations (Mar. 22, 2023), https://www.sec.gov/news/press-release/2023-59.
[65] Steven Mark Levy, Regulation of Securities: SEC Answer Book, What is Regulation S? (5th ed. 2021)
[66] See Morrison v. Nat'l Australia Bank Ltd., 561 U.S. 247 (2010)

listed on domestic exchanges," or (ii) enter into "domestic transactions in other securities." While the first prong is generally straightforward analyzed, determining whether a transaction is "domestic" is not always so clear cut.

The application of *Morrison* has varied in the case of crypto assets. For example, in In *re Tezos Securities Litigation*, the Northern District of California held that sales of digital tokens to persons located in the U.S., hosted on a U.S. server, with participants in the ICO being located in the U.S., and almost exclusively marketed to U.S. residents was sufficiently "domestic." The court also noted that the ICO "became irrevocable only after it was validated by a network of global "nodes" and such nodes were clustered more densely in the United States than in any other country."[67] However, the Southern District of New York in *Williams v. Block one* found that the location of the purchasers or title passing over servers located in the U.S. were not controlling factors and instead focused on the initial validation of the first node. The court reasoned that the transactions became "irrevocable" when the transaction was validated by the first node, and thus the location of the first node to validate the transaction was what mattered.[68]

E. Securities Trading Systems

1. Definition of an Exchange and Proposed Amendment

The Commission recognizes national securities exchanges that have been registered with the Commission under Section 6 of the Exchange Act.[69] Each exchange is a self-regulatory organization with its own set of "listing standards." The most recognizable such exchanges are Nasdaq and the NYSE. If an issuer lists its securities on such an exchange, the issuer will be subject to the regulations and standards created by the exchange. Unlisted companies and their securities may be traded through other marketplaces, such as the OTC Markets Group, which have their own separate requirements.

---

[67] 7-6779 - In Re Tezos Securities Litigation, https://www.govinfo.gov/app/details/USCOURTS-cand-3_17-cv-06779/context.

[68] See Williams v. Block one, No. 20-CV-2809 (LAK), 2022 WL 5294189 (S.D.N.Y. Aug. 15, 2022)

[69] 15 U.S.C. § 78a (The current definition of an exchange in the regulations under the Exchange Act is: "(a) An organization, association, or group of persons shall be considered to constitute, maintain, or provide "a market place or facilities for bringing together purchasers and sellers of securities or for otherwise performing with respect to securities the functions commonly performed by a stock exchange," as those terms are used in section 3(a)(1) of the Act, (15 U.S.C. 78c(a)(1)), if such organization, association, or group of persons:
(1) Brings together the orders for securities of multiple buyers and sellers; and
(2) Uses established, non-discretionary methods (whether by providing a trading facility or by setting rules) under which such orders interact with each other, and the buyers and sellers entering such orders agree to the terms of a trade.").

On January 26, 2022, the SEC proposed amendments regarding the definition of "exchange." The proposed change expands the definition to include systems that offer the use of non-firm trading interest and communication protocols to bring together buyers and sellers of securities.[70] The amendment would reference "trading interest," instead of "orders" as the basis on which to regulate trading systems and would encompass many digital asset industry participants by including a group of persons who make available "communication protocol systems" that allow people to express interest in potential securities trades. The proposed amended text is below (newly proposed text underlined):

"(1) brings together buyers and sellers of securities using trading interest; and

(2) makes available established, non-discretionary methods (whether by providing a trading facility or communication protocols, or by setting rules) under which buyers and sellers can interact and agree to the terms of a trade."

The proposal would explicitly seek to absorb decentralized finance (DeFi) into the requirements of the regulations of SEC rules and oversight. DeFi is often seen as the crypto asset version of Wall Street, as DeFi protocols aim to provide financial services such as borrowing, lending, trading and other without the need of centralized, established institutions such as brokerages and banks. DeFi protocols allow users to access blockchain-based smart contracts to execute transactions when certain conditions are met. It is unclear how the revised definition of "exchange" would impact various DeFi protocols. It is notable that, despite a successful enforcement action against it by the Commodities Futures Trading Commission, the protocol overseen by Ooki DAO, which allows users to execute leveraged derivatives trades, continues to operate as it had prior to the regulatory action.[71]

2. The Role of Transfer Agents

Transfer agents are entities which play the middleman between issuing companies and security holders. They play a critical role to the successful completion of secondary securities trades since they record changes of ownership, issue and cancel certificates, maintain securities registers, maintain the issuer's security holder records and distribute dividends. Federal securities laws require that transfer agents be registered with the Commission. The proliferation of crypto assets has created a need for transfer agents in the crypto space and regulated securities tokens that are issued and traded on blockchain networks also require transfer agents to facilitate the completion of trades between issuers and investors.

---

[70] Commissioner Caroline A. Crenshaw, Statement on Amendments to Exchange Act Rule 3b-16, Regulation ATS, and Regulation SCI (Jan. 26, 2022), https://www.sec.gov/news/statement/crenshaw-ats-20220126.

[71] See Coin Market Cap, https://coinmarketcap.com/currencies/ooki-protocol/#About (last visited Dec. 28, 2023).

A notable example of a digital securities transfer agent is Securitize, backed by Coinbase, which was registered on August 21, 2019, by the Commission.72

3. Alternative Trading Systems

Alternative Trading Systems (ATS) are trading systems that fall under the definition of an "exchange" within the federal securities law but not required to register as a national securities exchange under the Rule 3a1-1(a) exemption of the Exchange Act. On July 8, 2019, the Commission and the Financial Industry Regulatory Authority (FINRA) issued compliance guidance under current custody regulations for broker-dealers operating using blockchain technology. In the guidance, FINRA provided an example with a four-step process involving an ATS. The process for compliant trades would be[73]:

1. the buyer and seller send their respective orders to the ATS;
2. the ATS matches the orders;
3. the ATS notifies the buyer and seller of the matched trade; and
4. the buyer and seller settle the transaction bilaterally, either directly with each other or by instructing their respective custodians to settle the transaction on their behalf.

The result would be that the alternative trading system would not guarantee or otherwise have responsibility for settling the trades and would not exercise any level of control over the digital asset securities. As a result, concerns grew about potential operational and settlement risks associated with the process. In response, on September 25, 2020, the Commission issued a no-action letter to FINRA confirming that the Commission would take no enforcement action against broker-dealers trading digital asset securities that followed the following three-step process[74]:

1. the buyer and seller send their respective orders to the ATS, notify their respective custodians of their respective orders submitted to the ATS, and instruct their respective custodians to settle transactions in accordance with the terms of their orders when the ATS notifies the custodians of a match on the ATS;
2. the ATS matches the orders; and

---

[72] See Ana Alexandre, US SEC Registers Digital Securities Platform Securitize as Transfer Agent, Cointelegraph (August 21, 2019), https://cointelegraph.com/news/us-sec-registers-digital-securities-platform-securitize-as-transfer-agent.

[73] Joint Staff Statement on Broker-Dealer Custody of Digital Asset Securities (July 8, 2019), https://www.sec.gov/news/public-statement/joint-staff-statement-broker-dealer-custody-digital-asset-securities.

[74] ATS Role in the Settlement of Digital Asset Security Trades (Sept. 25, 2020), https://www.sec.gov/divisions/marketreg/mr-noaction/2020/finra-ats-role-in-settlement-of-digital-asset-security-trades-09252020.pdf.

3. the ATS notifies the buyer and seller and their respective custodians of the matched trade and the custodians carry out the conditional instructions.

In addition to the three-step process describe above, the SEC required the following from the broker-dealer operator of the ATS[75]:

1. The broker-dealer operator maintains a minimum of $250,000 in net capital;
2. The agreements between the broker-dealer operator and its customers clearly state that the broker-dealer operator does not guarantee or otherwise have responsibility for settling the trades;
3. The broker-dealer operator has established and maintains reasonably designed procedures to assess whether a digital asset security was offered and sold initially pursuant to an effective registration statement or an available exemption from registration, and whether any secondary transactions of the digital asset security on or through the ATS are made pursuant to an effective registration statement or an available exemption from registration; and
4. The transactions in digital asset securities otherwise comply with the federal securities laws.

F. The Regulation of Investment Companies

Generally, an investment company is a company which engages in the business of investing in the securities of other companies. The term investment company can also include any company whose investment securities comprise at least 40% of their total assets. Common examples of investment companies include open-end management companies or mutual funds.

1. Registered and Private Investment Funds

As a general rule, an investment company may not do business unless it is registered under the Investment Company Act of 1940 or is within the exemptions under the Investment Company Act. For an investment company to be registered under the Investment Company Act it must provide the Commission a notification and within 3 months of filing such notification, must also file a registration statement with the required disclosures. The Investment Company Act requires significant ongoing disclosures from registered investment companies, expanding disclosure provisions that were already applicable to the investment company industry under the Securities Act and the Exchange Act. The Investment Company Act also requires investment companies to have a similar structure to a standard corporate form including having a

[75] *Id.*

board of directors and independent directors both to oversee the investment company's operation.[76]

On May 11, 2021, the Commission issued a "Staff Statement on Funds Registered Under the Investment Company Act Investing in the Bitcoin Futures Market." The statement covered mutual funds' interests in Bitcoin futures and stated that it would closely monitor and assess mutual funds' and investment advisers' ongoing compliance with the Investment Company Act, including analyzing the liquidity and depth of companies' holdings in Bitcoin futures in addition to potential fraud and manipulation.[77]

There are certain exemptions to registration under Section 3(c) of the Investment Company Act for private investment funds. A privately held investment company can avoid regulation if the company: (i) does not make or propose to make a public offering of its securities and (ii) must not have more than 100 beneficial owners of its securities. Another option is under Section 3(c)(7). Section 3(c)(7) provides for a similar exemption except the second prong allows for the company's outstanding securities to be exclusively owned by qualified purchasers. A qualified purchaser is any individual with an investment portfolio valued at $5 million or greater[78].

2. Inadvertent Investment Companies

Companies that may not intend to be an investment company may run up against the second definition under the Investment Company Act if investment securities comprise more than 40% of their total assets. Typical scenarios include operating companies with strong equity investing in equity securities, investing a substantial portion of their assets in securities of subsidiaries that are less than majority-owned, or investing in high quality debt securities. Companies that have significant crypto asset holdings which, in combination with other securities holdings, would constitute more than 40% of their assets should be aware that they may be considered to be investment companies if such assets are found to be securities.

G. Brokers and Dealers

The Exchange Act requires all "brokers" and "dealers" to register with the SEC and to join a self-regulatory organization. As a result, it is vital to understand when a person made be considered a broker or dealer under the Exchange Act.

---

[76] See 15 USCA § 80a-17, https://www.govinfo.gov/content/pkg/COMPS-1879/pdf/COMPS-1879.pdf ("Investment Company Act")

[77] See Staff Statement on Funds Registered Under the Investment Company Act Investing in the Bitcoin Futures Market (May 11, 2021), https://www.sec.gov/news/public-statement/staff-statement-investing-bitcoin-futures-market.

[78] See Investment Company Act.

1. Definition of "Broker"

The Exchange Act defines the term broker as "a person engaged in the business of effecting transactions in securities for the account of others."[79] Determining who may be considered a broker can be a difficult task since the elements of the definition are not defined by the Exchange Act. Courts have looked at the term "engaged in the business" to critically mean that a person's receipt of transaction-based compensation is a "hallmark of broker-dealer activity."[80] The Commission has also looked to other factors such as the regularity of engaging in the activity and the handling of customer funds and securities.

The Commission and the courts take a broad view in determining what is considered "effecting transactions in securities." Some factors identified by the courts that are helpful to determining when a person is affecting transactions in securities include (i) participating in structuring a transaction, (ii) actively and aggressively seeking purchasers, (iii) soliciting transactions, (iv) participating in negotiations, (v) valuing the merits of or recommending an investment and (vi) taking and executing orders. These factors involve participating in the key points in the chain of distribution and thus "effecting" a transaction in securities.[81]

2. Definition of "Dealer"

The Exchange Act defines a dealer as "any person engaged in the business of buying and selling securities (not including security-based swaps, other than security swaps with or for persons that are not eligible contract participants) for such person's own account through a broker or otherwise." Therefore, to be considered a dealer a person must be in the business of proprietary trading or market making. The term excludes persons "that buy or sells securities (not including security-based swaps, other than security-based swaps with or for persons that are not eligible contract participants) for such person's own account, either individually or in a fiduciary capacity, but not as a part of a regular business."

In early 2022, the Commission proposed Exchange Act Rule 3a5-4 to expand the definition of "dealer." The definition would now include persons engaged in a routine pattern of buying and selling securities (or government securities) for their own account that has the effect of providing liquidity to other market participants. The proposed Rule 3a5-4 highlighted three types of activities that would fall under this new definition including: (i) routinely making roughly comparable purchases and sales of the same or substantially similar securities (or government securities) in a day; or (ii) routinely expressing trading interests that are at or near the best available prices on both sides of

---

[79] 15 U.S. Code § 78c. Definitions and application.
[80] Denial of No-Action Request, Brumberg, Mackey & Wall, P.L.C. (May 17, 2010), https://www.sec.gov/divisions/marketreg/mr-noaction/2010/brumbergmackey051710.pdf.
[81] See SEC v. Kramer, 778 F. Supp. 2d 1320 (M.D. Fla. 2011).

the market and that are communicated and represented in a way that makes them accessible to other market participants; or (iii) earning revenue primarily from capturing bid-ask spreads, by buying at the bid and selling at the offer, or from capturing any incentives offered by trading venues to liquidity-supplying trading interests. Furthermore, the Commission proposed Exchange Act Rule 3a44-2, which provides a quantitative standard that expands the definition of dealer to include any person who, in four of the last six calendar months, bought or sold over $25 billion in government securities to register as a government securities dealer.[82]

The proposed definition has implications for liquidity providers under the frameworks of various DeFi protocols, DEXs and automated money markets. Among the most obvious issues is the decentralized nature of these frameworks. It is not immediately clear who or what would be registered and whose responsibility it would be carry out that registration. All of these are simply code deployed to a blockchain network and "called" by users, with the main selling point that they operate without the need for any intermediary entities or the risks and costs they bring.

3. The Registration Requirement for Broker-Dealers

While there are a few exceptions, Section 15(a)(1) of the Exchange Act generally requires broker-dealers to register with the Commission. Section 15(a)(1) makes it unlawful for any broker or dealer to use the mails (or any other means of interstate commerce) to "effect any transactions in, or to induce or attempt to induce the purchase or sale of, any security" unless the broker-dealer has registered with the Commission in accordance to Section 15(b) of the Exchange Act.[83] If a broker-dealer does not qualify for any of the exemptions, the broker-dealers must registered by filing an application on Form BD. The form also allows for the broker-dealer to apply for membership in a self-regulating organization, typically FINRA or a registered national securities exchange. FINRA is a not-for-profit organization authorized by Congress that oversees U.S. broker-dealers. FINRA's role, similar to the Commission, is to ensure that investors are protected by making sure the broker-dealer industry operates fairly and honestly. FINRA ensures that (i) investors receive complete disclosure about the investment product, (ii) securities product advertisements are truthful and not misleading and (iii) any securities product sold to an investor is suitable for that investor's needs.

H. Clearing Agencies

Section 17A of the Exchange Act, Rule 17Ab2-1 and Form CA-1 require entities that intend to provide clearing agencies services to register with the Commission or obtain

[82] See SEC Proposes Rules to Include Certain Significant Market Participants as "Dealers" or "Government Securities Dealers" (Mar. 28, 2022), https://www.sec.gov/news/press-release/2022-54.
[83] 15 U.S. Code § 78o. Registration and regulation of brokers and dealers.

an exemption from registration. The term clearing agency is broadly defined that includes any person who acts as an intermediary in making payments and/or deliveries in connection with transactions in securities, acting functionally as the buyer to every seller and the seller to every buyer. The definition also includes any person, such as a securities depository, who (i) acts as a custodian of securities in connection with a system for the central handling of securities whereby all securities of a particular class or series of any issuer deposited within the system are treated as fungible and may be transferred, loaned, or pledged by bookkeeping entry without physical delivery of securities certificates, or (ii) otherwise permits or facilitates the settlement of securities transactions or the hypothecation or lending of securities without physical delivery of securities certificates.[84] The most notable example of a registered clearing agency is The Depository Trust Company ("DTC"). As previously discussed in this chapter, the DTC is a central securities depository that manages book entry securities. It was established in 1973 to reduce costs and provide clearing and settlement efficiencies by making "book-entry" changes to ownership of the securities. It provides record-keeping in electronic form and provides settlement services for almost all securities in the U.S. including, equity, corporate and municipal bonds, mutual funds, derivatives and money market securities[85].

Paxos No- Action Letter. On October 25, 2019, Paxos Trust Company, LLC ("Paxos") requested no-action relief to the Commission regarding Paxos' operation of a securities settlement system. The Paxos settlement system is a private, permissioned blockchain that allows participants to settle securities trades directly with each other. It provides the option to settle on the standard settlement cycle of the second business day after the trade date (T+2), and also a shortened T+0 cycle. The blockchain would be Paxos' responsibility for updating with the addition of new blocks and the blocks could be reviewed and distributed to the participants in real time. The shortened settlement cycle and immediate access to settlement proceeds mitigates risk of financial losses due to any intervening causes that may occur between trade date and settlement date. In the letter, Paxos requested that they not be required to register as a clearing agency for a period of 24 months to operate the service to test the feasibility of the new securities settlement system. On October 28, 2019, Paxos was granted the no-action relief on the terms discussed by Paxos.[86]

---

[84] 15 U.S. Code § 78c. Definitions and application.

[85] See The Depository Trust Company (DTC), https://www.dtcc.com/about/businesses-and-subsidiaries/dtc (last visited Dec. 28, 2023).

[86] Clearing Agency Registration Under Section 17A(b)(1) of the Securities Exchange Act of 1934, Paxos Trust Company, LLC (Oct. 28, 2019), https://www.sec.gov/divisions/marketreg/mr-noaction/2019/paxos-trust-company-102819-17a.pdf.

I. Enforcement Issues

1. Investigations and the Subpoena Process

Under the Exchange Act, the Commission has the discretion to make any such investigations as the Commission deems necessary to determine whether an individual or business has violated, is violating or is about to be violating the Exchange Act or any rules issued under the Exchange Act.[87] Similarly, the Investment Company Act allows for the Commission to make any such investigations on whether any person has violated or is about to violate the Investment Company Act. Prior to any sort of investigation under the applicable Acts, it must "appear to the Commission, either upon complaint or otherwise, that the provisions of [the Act or any Rule thereunder] have been or are about to be violated." Further, each of the major federal securities acts have provisions that allow for the Commission to subpoena individuals and companies based on these investigations.[88] The Commission's subpoena powers are substantially identical to its powers under Section 21(b) of the Exchange Act which provides:

"For the purpose of any such investigation, or any other proceeding under this title, any member of the Commission or any officer designated by it is empowered to administer oaths and affirmations, subpoena witnesses, compel their attendance, take evidence, and require the production of any books, papers, correspondence, memoranda, or other records which the Commission deems relevant or material to the inquiry. Such attendance of witnesses and the production of any such records may be required from any place in the United States or any State at any designated place of hearing."

This subpoena power extends nationwide for all of the major securities laws acts and the Commission may enforce its subpoenas by applying to the applicable U.S. district court. Should a person fail to obey the court order, they may be found in contempt.[89]

2. Section 5 Violations

As previously discussed, Section 5 of the Securities Act requires any sale or offer to sell a security in the United States to be made pursuant to an effective registration statement unless an exemption applies. Section 5 violations are strict liability, meaning that there is no requisite mental state or intent for finding a person liable. The liability extends to each participant of the sale who was necessary for the transaction or who was a substantial factor in bringing it about. In determining the appropriate penalty for

---

[87] 15 U.S.C. § 78a.
[88] See U.S. Securities and Exchange Commission, Laws and Rules (May 13, 2020), https://www.sec.gov/investment/laws-and-rules.
[89] 15 U.S.C. § 78a.

the violation, courts may consider (i) the egregiousness of the conduct, (ii) the degree of scienter, (iii) whether the action created substantial losses or a risk of substantial losses to the other persons, (iv) whether the violation was an isolated incident or recurring, (v) admission of wrong doing and (vi) the current and future financial condition of the defendant.[90] As a remedy, the district court has broad discretion in determining whether or not to order disgorgement (the giving up of any profits made as a result of the violating activity) and to calculate the amount to be disgorged. Section 12(a)(1) also provides a remedy for purchasers to sue issuers for offering or selling non-exempt security, so long as the purchaser can prove a direct link between the purchaser and the seller. The purchaser may obtain as a remedy either the rescission of the purchase with interest or damages should the investor have sold the securities for less than initially purchased.[91]

3. Section 10(b) and Rule 10b-5 Violations

Section 10(b) of the Exchange Act and Rule 10b-5 provide the baseline antifraud provisions in federal securities law by prohibiting material misrepresentations and misleading omissions in connection with the purchase or sale of securities. Section 10(b) makes it unlawful for any person, directly or indirectly, through the use of any means, instrumentality of interstate commerce, mail, or any facility on a national securities exchange "to use or employ, in connection with the purchase or sale of any security registered on a national securities exchange or any security not so registered, or any securities-based swap agreement, any manipulative or deceptive device or contrivance in contravention of such rules and regulations as the Commission may prescribe as necessary or appropriate in the public interest or for the protection of investors." [92] Rule 10b-5 further makes it unlawful for any person, directly or indirectly, in connection with the purchase or sale of any security, to (i) employ any device, scheme, or artifice to defraud, (ii) make any untrue statement of a material fact or to omit to state a material fact necessary in order to make the statements made, in the light of the circumstances under which they were made, not misleading, or (iii) engage in any act, practice, or course of business which operates or would operate as a fraud or deceit upon any person.[93] Rule 10b-5 reinforces the main purpose of the federal securities laws in requiring fair and full disclosure. For a private plaintiff or the Commission to prove a violation of Rule 10b-5, they must prove the following elements: (i) the individual misrepresented a material fact, (ii) the individual made that misrepresentation knowingly, (iii) the plaintiff relied on the individual's material misrepresentation and (iv) the plaintiff suffered loss. One of the more difficult elements to prove is determining whether the individual misrepresented or omitted a "material" fact. Facts

[90] SEC v. Gann, 565 F.3d 932, 940 (5th Cir. 2009).
[91] 15 U.S.C. § 77a.
[92] 15 U.S.C. § 78j. Manipulative and deceptive devices.
[93] 17 CFR § 240.10b-5. Employment of manipulative and deceptive devices.

may be considered material if there is a substantial likelihood that an investor would consider the fact important in their decision for investing or voting. As such, the materiality of a fact depends on the significance the "reasonable investor" would place on withheld or misrepresented information; that is, would a reasonable investor have changed their investment decision had the information been disclosed? The Commission has no bright line test for materiality and the analysis must be made on the totality of information available in each specific case.

4. Market Manipulation

Section 10(b) of the Exchange Act also makes it unlawful for the use of "any manipulative... device or contrivance" in violation of the federal securities laws. Although not expressly defined in the Exchange Act, the term manipulation has been developed over time through the courts.[94] Courts have viewed manipulation in the securities realm as being practices that mislead investors by artificially affecting the market done with the intention to deceive investors through the controlled price. Market manipulation does not cover legitimate speculation of future trends and economic directions. In addition, market manipulation does not cover arbitrage, in which investors may take advantage of a securities disparity between markets by buying the same securities in one market and selling them at a potentially higher price at another market.

In the crypto space, users of DeFi protocols and DEXs can seek to maximize their returns through the use of techniques generally referred to as "maximal extractable value" ("MEV"). Depending on how MEV activity is structured, it may result in market manipulation activity. The current crypto currency systems currently require pending transactions to be held in a "mempool" which is the public memory pool before they are into a block and added to the blockchain. This mempool is public and market participants employing bots known as "MEV searchers" may be able to take advantage of potential profits by re-ordering transactions, censoring transactions or creating new transactions based on the pending transactions in the mempool. Although some opportunities do not fall under market manipulation, such as MEV searchers using bots to locate arbitrage opportunities between DEXs, other techniques such as "front-running" and "sandwich attacks" may be deemed to be manipulative. Front-running is where the MEV searcher replicates profitable DEX transactions that they have found from legitimate traders. The MEV searcher provides for higher fees to go to the miners, prompting miners to choose to validate the front-runners' transaction over the legitimate DEX trader. Sandwiching allows MEV searchers to use MEV bots to search the mempool for large pending trades in the DEX. Once found, the searcher will place a trade using the same token immediately before and another after the large pending trade, essentially sandwiching the large pending trade, which raises the price of the

[94] See 17 CFR 240.10b-5

token in question prior to the pending trade and selling all of the tokens after the pending trade. In both instances, the legitimate DEX trader pays a higher rate prior to entering into the blockchain due to the MEV searcher bots.[95]

5. Insider Trading

Insider trading refers to the buying or selling of a security while the individual trading has access to material nonpublic information ("MNPI") about the security. While insider trading is generally illegal, in certain circumstances limited activities are permitted, the most common example of which being when a transaction of securities is made on behalf of an executive or employee holding MNPI pursuant to a pre-existing administered plan to buy or sell stock. Insider trading is illegal when the security is sold with a breach of fiduciary duty or other relationship of trust on the basis of the material nonpublic information about that security or its issuer. The fiduciary duty extends to the issuer, the issuer's shareholders and to any person who is the source of the MNPI. The materiality standard is the same as in Rule 10b-5: Nonpublic information is information not broadly disseminated to the investing public generally. The public dissemination also cannot favor any special person or group. Typically, information will no longer be considered nonpublic when the information has been "fully impounded into the price of the particular stock."[96] Common examples of insider trading cases are (i) corporate officers, directors and employees trading after learning significant corporate developments, (ii) friends or family members trading after receiving insider information from corporate officers, directors and employees, (iii) third party service providers (including law firms, bankers, broker and printing firms) based on information obtained in connection with the services provided and (iv) government employees based on confidential information learned from employment.[97]

On May 30, 2023, the Commission announced that it had settled insider trading charges brought against Ishan Wahi, a former product manager at the exchange platform Coinbase. The charges were filed on July 21, 2022. In the complaint the Commission alleged that that Wahi "repeatedly tipped the timing and content of upcoming listing announcements" regarding crypto assets to be made available for trading on Coinbase to his brother and to his friend. Wahi, his brother and his friend were alleged to have purchased crypto assets on this knowledge and sold shortly after the announcements were made public. Wahi was concurrently charged by the

---

[95] See Mikołaj Barczentewicz, MEV on Ethereum: A Policy Analysis, International Center for Law & Economics (Jan. 23, 2023), https://laweconcenter.org/resources/mev-on-ethereum-a-policy-analysis/?doing_wp_cron=1691430775.4427149295806884765625.

[96] SEC v. Mayhew, 121 F.3d 44, 50 (2d Cir. 1997).

[97] Investor.gov, Insider Trading, https://www.investor.gov/introduction-investing/investing-basics/glossary/insider-trading (last visited Dec. 28, 2023).

Department of Justice (DOJ) with wire fraud and sentenced to 24 months in prison and disgorgement of certain crypto assets.[98]

6. Wire Fraud and Crypto Transactions

Beyond Commission enforcement and private litigation enabled by the securities laws, the DOJ has, as discussed above with respect to Ishan Wahi, recently been using the wire fraud statute to prosecute individuals for insider trading in crypto assets. The wire fraud statute prohibits any person engaging in interstate wire, radio or television communication for the purpose of knowingly participating in a scheme to defraud. As it does not require the assets involved in the scheme to be securities, enforcement action through this approach sidesteps the issue of determining whether crypto assets are securities.

In addition to the wire fraud charges the DOJ brought against Wahi, Nathaniel Chastain, a former product manager at Ozone Networks, Inc., was charged with wire fraud in a scheme to commit insider trading in NFTs in the first-ever insider trading case involving crypto assets. By charging Chastain with wire fraud, as opposed to securities fraud, the DOJ was able to avoid the need to determine whether the NFTs were securities. The DOJ focused on the scheme that Chastain had used to gain $57,000 dollars in profit from misappropriated information. Chastain had information related to what NFTs were going to be featured on OpenSea's homepage prior to their posting. Generally, the NFTs that were featured on OpenSea's homepage increased in price. The DOJ argued that because OpenSea employees were obliged to keep this information confidential and use it only for the benefit of OpenSea, Chastain misappropriated that information for personal financial gain and defrauded OpenSea as he purchased the NFTs prior to them being posted on OpenSea's homepage and then sold them after their posting. Chastain was convicted by a jury of wire fraud and money laundering on May 3, 2023.[99] The results of the trial likely will spur on the DOJ to continue using the wire fraud statute as a means to combat insider trading in the crypto asset market space without needing to determine whether such crypto assets are securities. The DOJ's action demonstrates that even if crypto assets may not be securities, wrongdoing would not necessarily go unpunished, perhaps contrary to the Commission's narrative that their regulation (so far, primarily through enforcement) of crypto assets is necessary for the protection of the public.

[98] See Former Coinbase Manager and His Brother Agree to Settle Insider Trading Charges Relating to Crypto Asset Securities (May 30, 2023), https://www.sec.gov/news/press-release/2023-98.
[99] See United States v. Chastain, 22-CR-305 (JMF) (S.D.N.Y. Oct. 21, 2022).

7. Remedies

There are several remedies available to the Commission for violations of the federal securities laws. The traditional remedy instituted by the Commission has been injunctive relief. In combination with its investigation powers, the Commission may also bring its own injunctive action. For an injunctive action the Commission must show a "reasonable likelihood" that, absent the ordering of the injunctive relief, the defendant will continue to engage in future violations. Factors include the nature of the violation, degree of scienter, recurring nature of the violations, a defendant's opportunity to continue future violations, a defendant's sincerity and assurances against future wrongdoing, good-faith reliance on counsel, collateral consequences resulting in the injunction and the lapse of time since the injunction. In addition to injunctive relief, the Commission has been successful in obtaining other ancillary relief, including monetary penalties, barring an individual from an officer or director position, disgorgement, and referral to state and federal authorities for civil or criminal proceedings. Typically, the Commission procures civil money penalties in enforcement actions that are settled, but the Commission has also received such relief in litigated cases as well. They may also impose money penalties in cease-and-desist proceedings. The Commission has also been able to achieve remedies such as restructuring corporate boards and ordering officer or director bars for individuals if their conduct demonstrates an "unfitness" to serve in such capacity. Additional relief includes disgorgement of "ill-gotten" gains, mandating accounting in administrative proceedings and asset freezes. Finally, the Commission may also refer matters and the relevant evidence related to those matters to state and other federal authorities to begin the process for civil and criminal proceedings. In addition, should any individual be uncooperative with the above process, the Commission may also initiate civil and criminal contempt proceedings against the officer or director.[100]

J. SEC's Accounting Authority – SAB 121 and Crypto Asset Custody

Another major power that the Commission has under Section 19(a) is to prescribe the information to be included in and the methods to be followed in the preparation of an issuer's accounts. In addition to the rules laid out in Regulation S-X, the Commission may from time to time issue Staff Accounting Bulletins which reflect staff's views regarding accounting disclosure.

On March 31, 2022, the SEC published a Staff Accounting Bulletin No. 121 ("SAB 121") regarding the accounting of an entity's obligation to safeguard crypto-assets an

[100] See Securities Regulation (LJP) § 12.01 (lexis.com).

entity holds for platform users,[101] which was effective as of April 11, 2022. In SAB 121, the SEC identified hypothetical companies that the guidance would apply to with the following characteristics:

1. Entity A's business includes operating a platform that allows its users to transact in crypto-assets;
2. Entity A also provides a service where it will safeguard the platform users' crypto-assets, including maintaining the cryptographic key information necessary to access the crypto-assets;
3. Entity A also maintains internal recordkeeping of the amount of crypto-assets held for the benefit of each platform user;
4. Entity A secures these crypto-assets and protects them from loss or theft, and any failure to do so exposes Entity A to significant risks, including a risk of financial loss;
5. The platform users have the right to request that Entity A transact in the crypto-asset on the user's behalf (e.g., to sell the crypto-asset and provide the user with the fiat currency (cash) proceeds associated with the sale) or to transfer the crypto-asset to a digital wallet for which Entity A does not maintain the cryptographic key information. However, execution and settlement of transactions involving the platform users' crypto-assets may depend on actions taken by Entity A.

The Commission noted that an affected entity should account for the safeguarding obligations as a liability on the entity's balance sheet, while simultaneously recognizing an asset related to the liability. The entity should disclose within its financial statements (i) clear disclosure of the nature and amount of crypto-assets that the affected entity is responsible for safeguarding, (ii) with separate disclosures for each significant crypto-assets; (iii) detail any vulnerabilities of the affected entity due to the concentration in such activities, (iv) disclosures regarding fair value measurements and (v) a description of the accounting of the safeguarding liabilities and corresponding assets. The Commission also noted that disclosures outside of the financial statements may also be required. Affected sections that may need additional disclosure includes the business section, risk factors and management's discussion and analysis of financial condition and results of operations (MD&A) sections of an affected entity's 34 Act filings. If material such disclosure should include: (i) the risk of discontinuation of such services, litigation, reputational harm ore regulatory enforcement, (ii) analysis on the legal ownership of the crypto-assets held for the platform users, specifically whether such assets would be available to satisfy creditor claims in the event of an affected entity's bankruptcy, and (iii) the potential effect that loss, theft or other unavailability of cryptographic key information could have on the affected entity's business, financial condition or results of operation.

[101] Securities and Exchange Commission, Staff Accounting Bulletin No. 121 (Apr. 11, 2022), https://www.sec.gov/oca/staff-accounting-bulletin-121.

Commodities Regulation

Kathryn Trkla and Michael Frisch*

A. Overview of CEA and CFTC Jurisdiction

1. Introduction

Derivatives play an important role in promoting healthy, transparent, and liquid markets in financial products, and derivatives on digital assets are no exception. Around the world, derivatives markets in cryptocurrency dwarf "spot" cash markets in volume and liquidity. Speculators and hedgers are drawn to derivatives markets for their capital efficiency and usefulness in pricing and transferring risk. But along with their usefulness comes risk. Typically, derivatives markets promote trading on margin, *i.e.*, with leverage, and small price movements in the underlying asset can lead to large losses for investors. American policymakers learned hard lessons about derivatives markets over decades of experience, resulting in the comprehensive (and at times complicated) regulatory system in place today in the United States. Derivatives based on digital assets on a blockchain are a relative newcomer to that age-old system.

The Commodity Futures Trading Commission (CFTC or Commission) is the federal agency that is authorized under the Commodity Exchange Act (CEA), 7 U.S.C. § 1, *et seq.*, to oversee and regulate most segments of the derivatives markets in the U.S., which today includes futures, options on futures, commodity options and swaps. The Securities and Exchange Commission (SEC), though, is responsible for regulating certain (but not all) derivatives markets that involve securities. The CFTC also regulates certain leveraged "retail commodity transactions" that are not necessarily derivatives. The CFTC's mission is to implement and enforce the CEA and thereby to promote the integrity, resilience, and vibrancy of the U.S. derivatives markets within its remit.

The CEA's reach is largely delineated by what is a "commodity." The CEA's definition is broad and extends beyond what one would commonly think of as a commodity, for example it covers securities, stock indices and foreign currencies, but

* Trkla is a Partner at Foley & Lardner (see https://www.foley.com/people/trkla-kathryn-m/), Chicago, IL. Frisch is a Partner at Croke Fairchild Duarte & Beres (see https://crokefairchild.com/team/michael-frisch/). Louis Goldman, Managing Partner of the Navigator Law Group LLC, reviewed this chapter.

the definition is not limitless. The CFTC's position is that many digital assets, certainly bitcoin and Ethereum but also other digital assets including stablecoins, are "commodities" (of the non-security variety) under the CEA.

Pursuant to its authority under the CEA, the CFTC writes rules and supervises derivatives market activity and market participants, including exchanges, clearing organizations, large traders, and professional intermediaries such as those who assist with executing or clearing derivatives transactions or offer derivatives trading advice. The enforcement division of the CFTC investigates and brings cases for violations of the CEA and Commission regulations. The CFTC's enforcement division can also police fraud and manipulation concerning the trading, offer, or sale of commodities in interstate commerce, but the CFTC generally has no authority to regulate or write rules for such cash market trading of commodities including digital assets. Instead, the CFTC's *regulatory* jurisdiction (as opposed to its *enforcement* jurisdiction) with respect to cryptocurrencies is limited to futures or other derivatives and certain leveraged transactions involving such assets. That is why it is often said of the CFTC that "futures is our middle name."

The CEA's origins date back to 1922 and with the substantive amendments made over the decades its provisions today can seem complicated to navigate. From a big picture perspective, though, if a transaction involves a derivative on a digital asset or involves a digital asset that is itself a derivative (as we discuss further below) and members of the public may only engage in such transactions on a CFTC-regulated exchange and their transactions must be centrally cleared by a regulated clearing house. In contrast, if trading is limited to institutional investors known as "eligible contract participants" the trades may occur away from a regulated exchange but will be subject to other requirements that apply to swaps transactions.

Given the complexities of the CEA and its potential touch points with digital asset trading activities, it is important for any practitioner who deals with digital assets to at least have a high-level understanding of the CFTC's jurisdiction and powers, and the regulatory structure that governs most derivatives trading in the U.S.

Terminology: Digital Assets, Digitized Assets, Smart Contracts, etc.

This chapter uses the term "digital asset" in the specific sense of an electronic record in which a person has a right or interest, where the record itself is the item of value. It also uses the term generically to refer both to a digital asset in that specific sense and to a "digitized asset," *i.e.*, to a digitized record of ownership of an asset that exists apart from the electronic record, such as an electronic warehouse receipt representing title to a bar of gold or to a carbon emissions credit. Admittedly, the distinction between the two can become blurred, say for example by stablecoins that peg their value to a referenced foreign currency or other commodity (*e.g.*, gold) that a sponsor or foundation holds in reserve.

This chapter also in places covers "smart contracts" as a type of digital asset, defined as a digital asset with coded instructions that automatically execute when prescribed conditions are met. If the coded instructions functionally replicate or implement elements of a financial transaction, that can raise the issue whether the digital asset itself is a derivative within the CEA framework. For example, in the CFTC's recent enforcement action against ZeroEx, the Commission concluded that certain "leveraged tokens" which functionally provided leveraged exposure to other digital assets by automatically borrowing and trading stablecoins in other DeFi protocols, were *themselves* considered products subject to the CFTC's jurisdiction, even though no "buyer" or "seller" of a derivatives contract could be identified.[1] Typically derivatives like futures, options, and swaps have two (or more) counterparties. The ZeroEx case may be the first in which the CFTC concluded that a token itself could *embody* a derivative.

In keeping with the Web3 focus of this Reference Book, this chapter covers digital assets when they are represented on a distributed ledger or blockchain network. Digital assets could be represented on other types of electronic ledgers. Other systems have long existed for recording and transferring electronic warehouse receipts, shipping certificates or other documents evidencing title or a claim to an underlying commodity. Futures exchanges have for years listed derivatives contracts that provide for settlement upon expiration via transfer of the electronic record from the seller to the buyer through such systems. The discussion in this chapter, though, is from the perspective of how the CEA framework could apply to the combination of digital assets existing on a distributed ledger or blockchain network, which is the newer development.

This chapter sometimes uses the terms "virtual currency" or "cryptocurrency" to refer to digital assets or types of digital assets, as those are terms often used by others, such as the CFTC's use of "virtual currency." Whatever terms are used, the characteristics of a particular digital asset are more important than the label when evaluating whether or how trading of a digital asset could fall within the CEA framework.

There is of course, an issue whether a digital asset could be classified as a security, which other chapters cover. This chapter generally focuses on digital assets that are <u>not</u> securities. Similarly, except where otherwise called out, this chapter uses the terms "commodity" and "commodities" to refer to commodities that are <u>not</u> securities.

[1] See In re ZeroEx, Inc,, CFTC Docket No, 23-31 (Sept. 7, 2023).

2. Which Digital Assets are Commodities.

A threshold question is whether a digital asset is a commodity. For digital assets that reference other assets, the commodity analysis could apply to the digital asset, to the underlying reference or to both, for example a digital asset that is a stablecoin pegged to the value of a commodity or that contains coded instructions that execute automatically based on changes in the price or value of a commodity.

The CEA's definition of "commodity" is famously broad. As defined under § 1a(9) of the CEA, commodities, with limited exceptions, includes all manner of "other goods and articles, . . . and all services, rights, and interests . . . in which contracts for future delivery are presently or in the future dealt in."[2] *See Board of Trade of City of Chicago v. SEC*, 677 F.2d 1137, 1142 (7th Cir. 1982) ("This language was also meant to encompass futures markets that were expected to be expanded to cover non-traditional goods and services."), *vacated on other grounds*, 103 S.Ct. 434 (1982). Courts have recognized that the definition of "commodity" under the CEA is "broad." *Id.* Indeed, the breadth of the commodity definition is evidenced by the fact that Congress has carved out only onions and movie box office receipts from the commodity definition, in 1974 and 2010, respectively. 7 U.S.C. § 1a(9). (Each of those exclusions has its own backstory that is outside the scope of this Chapter.)

The definition of commodity is so broad it even covers securities. In lieu of excluding securities from the definition, Congress added provisions over the years to the CEA and federal securities laws that allocate jurisdiction between the CFTC and SEC over derivatives related to securities or a group or index of, or interest in, securities, as described below. This section pre-supposes that a digital asset is not a security, but there is not a sharp boundary between a non-security and security digital asset and the CFTC and SEC arguably have asserted contradictory claims of enforcement jurisdiction over the same digital asset or same type of digital asset as a non-security commodity and as a security.

Beginning in 2015, the CFTC has considered many digital assets to be commodities under the CEA (implicitly, of the non-securities variety). *See, e.g., CFTC v. McDonnell*, 287 F.Supp.3d 213, 228 (E.D.N.Y. 2018) ("Virtual currencies can be regulated by CFTC as a commodity. . . . They fall well-within the common definition of 'commodity' as well as the CEA's definition of 'commodities' as 'all other goods and articles . . . in which contracts for future delivery are presently or in the future dealt in.'"); *CFTC v. My Big Coin Pay, Inc.*, 334 F.Supp.3d 492, 495-98 (D. Mass. 2018) (denying motion to dismiss and determining that a non-bitcoin virtual currency is a "commodity" under the CEA); *In re Coinflip, Inc.*, CFTC No. 15-29, 2015 WL 5535736, *2 (Sept. 17, 2015) (consent order) ("Bitcoin and other virtual currencies are encompassed in the definition [of § 1a(9) of the CEA] and properly defined as commodities.").

[2] The statutory definition is open to interpretation, one of which is that the futures trading qualification applies to "services, rights, and interests" but not to "goods and articles."

The CFTC has not formally defined "virtual currencies" via regulation, preferring to proceed via enforcement actions and in court cases. The CFTC, however, adopted a broad definition of the term "virtual currency" for purposes of its final 2020 interpretive guidance, *Retail Commodity Transactions Involving Certain Digital Assets*.[3] We discuss this Guidance and the events leading up to it in Section F, below. In the context of that interpretation, virtual currency was referenced as:

- "a digital asset that encompasses any digital representation of value or unit of account that is or can be used as a form of 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."[4]

However, the CFTC noted that it did not intend to create a bright-line definition given the evolving nature of a virtual currency and, in some instances, its underlying public distributed ledger technology ("DLT" or "blockchain").

In recent years, much focus has been on whether certain digital assets are "commodities," subject to the jurisdiction of the CFTC in some fashion, or "securities" subject to the SEC's jurisdiction. As noted, securities are technically "commodities" under the CEA, but they are a special type of commodity. However, insofar as cash market spot trading is concerned, cash market trading of non-derivative securities is generally outside the CFTC's enforcement jurisdiction and is the purview of the SEC.

To date, the CFTC's assertion of jurisdiction over digital assets has included a broad range of assets. Bitcoin, Ethereum, Litecoin, and similarly functioning cryptocurrency tokens have all been found to be "commodities." In *CFTC v. My Big Coin Pay, Inc.*, 334 F.Supp.3d 492, 495-98 (D. Mass. 2018), a federal district court found that a digital asset that functioned similarly to bitcoin met the definition of a "commodity" under the CEA. It is reasonably well-settled that most fungible "cryptocurrencies," or similar tokens or digital assets would be considered to be "commodities."[5]

The CFTC also considers stablecoins to be commodities. In 2021, the CFTC resolved via consent order a case involving the stablecoin tether. *In re Tether Holdings Ltd.*, CFTC No. 22-04, 2021 WL 8322874 (Oct. 15, 2021) (consent order). Citing the broad statutory definition of a commodity and the CFTC's prior actions that found virtual currencies to fit the definition, it concluded that "[t]he USDt token, a virtual currency stablecoin, is a commodity and subject to applicable provisions of the Act and Regulations." 2021 WL 8322874 at *7. In March 2023, the CFTC asserted that the Binance stablecoin "BUSD"

---

[3] 85 Fed.Reg. 37,734 (June 24, 2020).

[4] *Id.* at 37,741

[5] See https://www.cftc.gov/PressRoom/PressReleases/7820-18#:~:text=Agreeing%20with%20the%20CFTC's%20arguments,that%20there%20is%20futures%20trading.

was a commodity in its enforcement action against Changpeng Zhao and Binance. *See CFTC v. Zhao et al*, 1:23-cv-01887 (N.D. Ill. March 27, 2023).

Interestingly, the SEC has also asserted that some stablecoins – namely BUSD – are securities. Just a few months after the CFTC sued Binance, the SEC brought its own case in the U.S. District Court for the District of Columbia (23-cv-01599) in which it alleged that BUSD was a security in part because it was sold as part of "a profit-earning scheme within the Binance ecosystem, touting returns for investors from simply buying BUSD or deploying it in Binance profit-generating programs."

Where the CFTC has asserted jurisdiction, the commodities typically are "fungible." Indeed, many courts have recognized that a quality inherent to commodities is that they are "fungible." *See, e.g. My Big Coin Pay, Inc.*, 334 F. Supp. 3d at 497; *CFTC v. UForex Consulting, LLC*, 551 F. Supp. 2d 513, 528 (W.D. La. 2008). A quantity of iron or corn is fungible, and thus can be freely traded in standardized contracts on open markets. Conversely, used cars, artwork, and houses are not "fungible." They each have their own unique characteristics that affect their utility and value. CFTC cases that have considered whether digital assets are "commodities" have focused on their fungible nature – one bitcoin is the same as another. *My Big Coin Pay, Inc.*, 334 F. Supp. 3d. at 497.

Accordingly, it is far less likely that digital assets that are not fungible like many NFTs would meet the CEA's definition of a "commodity" as applied by the CFTC. The same would seem to hold true for a digital asset that represents a specific piece of property in the metaverse.

3. The CFTC's Enforcement Jurisdiction

Much of this chapter concerns the CFTC's *regulatory jurisdiction* – the rules, regulations, and licenses needed to participate in the offer, sale, trading, and clearing of derivatives in the U.S. The CFTC's *regulatory* jurisdiction over derivatives is detailed and expansive. Notably, the CFTC also has general anti-fraud and anti-manipulation enforcement authority over cash markets for digital assets that are not securities, as commodities traded in interstate commerce. "Cash markets" denote the markets where the digital assets themselves are acquired, either in exchange for fiat money or other digital assets, as distinguished from markets for derivatives such as futures or options.

Importantly, the CEA does not give the CFTC authority to *regulate* cash commodity markets, meaning that the CFTC cannot and does not make rules and regulations governing how trading must occur on spot exchanges, and the CFTC does not make rules or set requirements for individuals who may sell cryptocurrencies to members of the general public, just as it does not make rules for the dealers of other "cash commodities," such as corn or oil.[6] That said, as discussed below, the CEA provides

[6] The CFTC, though, has authority to adopt rules for dealers within its jurisdiction that engage in the offer or sale of leveraged foreign currency transactions with members of the public, and adopted its Part 5 Regulations pursuant to that authority. The CEA's special provisions governing retail forex and the Part 5 Regulations do not apply to other commodities including virtual currencies.

that certain leveraged trading of commodities by retail customers must be treated "as if" the transactions are futures, which would bring the activity within the CFTC's authority to adopt rules and interpret CEA provisions.

Also, the CFTC does maintain authority to punish fraud or manipulation in any transaction involving commodities in interstate commerce, including virtual currencies (but excluding non—derivative securities). Section 6(c)(1) of the CEA, 7 U.S.C. § 9(1), is modeled after SEC Rule 10b-5 (17 C.F.R. § 240.10b-5) and states:

> It shall be unlawful for any person, directly or indirectly, to use or employ, or attempt to use or employ, in connection with any swap, or a contract of sale of any commodity in interstate commerce, or for future delivery on or subject to the rules of any registered entity, any manipulative or deceptive device or contrivance, in contravention of such rules and regulations as the Commission shall promulgate.

Under this authority, the CFTC promulgated Regulation 180.1 (17 C.F.R. § 180.1), which states in part:

> Prohibition on the employment, or attempted employment, of manipulative and deceptive devices.
>
> (a) It shall be unlawful for any person, directly or indirectly, in connection with any swap, or contract of sale of any commodity in interstate commerce, or contract for future delivery on or subject to the rules of any registered entity, to intentionally or recklessly:
>
> (1) Use or employ, or attempt to use or employ, any manipulative device, scheme, or artifice to defraud;
>
> (2) Make, or attempt to make, any untrue or misleading statement of a material fact or to omit to state a material fact necessary in order to make the statements made not untrue or misleading;
>
> (3) Engage, or attempt to engage, in any act, practice, or course of business, which operates or would operate as a fraud or deceit upon any person; or,
>
> (4) Deliver or cause to be delivered, or attempt to deliver or cause to be delivered, for transmission through the mails or interstate commerce, by any means of communication whatsoever, a false or misleading or inaccurate report concerning crop or market information or conditions that affect or tend to affect the price of any commodity in interstate commerce, knowing, or acting in reckless disregard of the fact that such report is false, misleading or inaccurate. Notwithstanding the foregoing, no violation of this subsection shall exist where the person mistakenly transmits, in good faith, false or misleading or inaccurate information to a price reporting service.

Using this authority, the CFTC has pursued numerous alleged virtual currency frauds, market manipulations, Ponzi schemes, pump-and-dumps, and more. A wide range of

fraud or fraud-based market misconduct involving digital assets could be prosecuted under this authority.

4. Overview of Derivatives and Other Transactions Regulated by the CFTC

A transaction in a digital asset that is within the scope of the CEA framework is subject to myriad statutory provisions and CFTC regulations. If such transactions are executed or offered out of compliance with these requirements that would be a violation of the CEA. The CFTC regulates many types of derivative transactions, imposing specific requirements on organized markets and clearing systems, industry professionals, and market participants. The CEA sets out separate statutory requirements for discrete market segments. Different sections of the CEA concern, for example, futures and options on futures contracts (7 U.S.C. § 6c(b)), options on commodities (7 U.S.C. § 2(a)(1)), and swaps (*Id.*).

The CEA's piecemeal approach reflects its history. Starting with its inception over 100 years ago as the Grain Futures Act of 1922, the statute had a rather targeted focus regulating organized exchange markets for futures contracts on agricultural commodities. Congress amended the CEA over the years, including notably in 1974 when it enacted the Commodity Futures Trading Commission Act to expand substantially federal regulation under the CEA to cover all domestic futures exchanges by expanding the commodity definition. (The 1974 amendments also established the CFTC as an independent federal agency with exclusive jurisdiction over the futures markets.)

For much of its history, the CEA's primary mission retained a laser focus on regulation and oversight of organized futures exchanges, with some limited special provisions added along the way addressing specific types of off-exchange trading of derivatives, such as commodity options. Things changed in 2010 with passage of the Wall Street Transparency and Accountability Act (Dodd-Frank Act). Title VII of the Dodd-Frank Act added extensive provisions to the CEA to establish a comprehensive regime for regulating institutional swaps markets; it also amended the federal securities laws to give the SEC jurisdiction to regulate trading activities in security-based swaps.

The CEA and CFTC regulations treat futures and options on futures together under the same regulatory regime. All futures contracts and options on futures contracts must be traded on or subject to the rules of a regulated exchange and are centrally cleared. Transactions in swaps are subject to very different regulatory requirements, among others the requirement that only institutional persons (eligible contract participants) may trade swaps away from a regulated exchange.

This dichotomy suggests that the CEA provides a clear delineation between derivatives that are futures or options on a futures, and derivatives that are swaps. Not so. The economic terms of futures contracts could fall within one of the prongs of the swap definition. When a derivative falls within that part of the Venn diagram, the

desired regulatory treatment may be a relevant consideration for deciding how to classify the transaction for CEA purposes. If parties do not want to trade on a regulated exchange, they could classify the transaction as a swap and comply with the regulatory requirements applicable to such transactions, including limiting trading counterparties to eligible contract participants. If broader market participation is desired, though, the transactions must occur on or subject to the rules of a regulated exchange and be cleared.

Futures and options on futures. The legal elements defining a futures contract for CEA purposes are found in the statute's grant of jurisdiction to the CFTC to regulate futures under CEA § 2(a)(1). Under that provision, futures are "contracts of sale of a commodity for future delivery." CEA § 1a(27). In general, when two parties execute a futures contract, they are entering into a promise or agreement to buy or sell a specified quantity of a particular underlying interest at a date in the future, at the price established at the time of the trade. Typically, parties trade futures for investment (speculation) or to hedge business risks, and not with the view to acquire the underlying commodity.

The CEA defines the term "future delivery" or more accurately what the term does not mean: the term does ***not*** include "any sale of any cash commodity for deferred shipment or delivery." This provision reflects the investment/hedging nature of futures trading, as distinguished from transactions where parties intend to buy or sell a commodity. The provision is the underpinning for the forward contract exclusion from regulation of deferred delivery contracts in commodities as futures contracts. Deferred delivery forward contracts are also excluded from regulation as swaps under the CEA when they involve a nonfinancial commodity (under a separate CEA provision, as interpreted by the CFTC).

Because futures may only legally be traded on or subject to the rules of a regulated exchange, it is useful to look at the contract terms and conditions that the exchanges establish for the contracts they list. Futures typically have standardized terms established by the exchanges, which are set out in the exchange's rulebook. The rules will identify the commodity covered by the futures contract, and any standardized terms for the commodity (*e.g.*, gold bars of a certain quality and weight). Such standardization can promote centralized, competitive trading in the markets the exchanges operate. Futures contracts can also have more tailored terms, though.

The exchange's rules will specify whether final settlement under the contract is accomplished by delivery of and payment for the underlying commodity (and the process for completing delivery) or by settling-up gains and losses via a cash payment. Exchanges typically list futures for trading for different expiration or delivery months with a specified last trading date and may list multiple expiration or delivery months concurrently for trading.

The term "option" is defined to include a contract that is "of the character of, or . . . commonly known to the trade as, an 'option', 'privilege', 'indemnity', 'bid', 'offer', 'put', 'call', 'advance guaranty', or 'decline guaranty.'" 7 U.S.C. § 1a(36). Under a typical

option, the holder, or buyer, pays a premium for the right to require the seller counterparty, often called the "writer," to sell an underlying interest to the option holder at a fixed strike price, in the case of a call option, or to purchase an underlying interest from the option holder at a fixed strike price, in the case of a put option. The option holder has an "exercise right" to decide whether to require its counterparty to sell the underlying interest to it or buy the underlying interest from it. That right, depending upon the contract terms, may be exercisable at any time through the term of the option, during a narrowly defined time-period at expiration of the contract, or under other terms.

The terms of the option may provide for automatic exercise when the strike price is "in-the-money," *i.e.*, when it is lower than the current market price at which the holder could buy the underlying interest under a call option, or higher than the current market price at which it could sell the underlying interest under a put option. As defined by its terms, the parties may settle their obligations upon exercise of an option on a commodity by delivery of the underlying commodity. The option terms could alternatively require the seller to make a cash payment for the difference between the strike price and the current market price or, in the case of a binary option structure, to pay a fixed amount.

An option on a futures contract, if exercised, typically settles into the underlying futures contract. Some options on futures, though, are structured to settle by cash payment when the strike price is in the money relative to the daily settlement price of the underlying futures contract.

As noted, futures and options on futures must be traded on or subject to the rules of a regulated exchange and are centrally cleared. Persons in the U.S. can legally trade futures and options on bitcoin and other virtual currencies at regulated exchanges, such as the Chicago Mercantile Exchange (CME), Coinbase Derivative, and Bitnomial Exchange. The trading of the products is monitored by the exchanges as industry self-regulatory organizations and by the CFTC.

Swaps. The term "swap" is defined in CEA § 1a(47) and CFTC Regulation 1.3. The definition is broad and covers many types of derivative structures, specifically:

1. Commodity Options: This prong of the definition covers puts, calls, caps, floors, collars, or similar options on the value of one or more interest rates or other rates, currencies, commodities, securities (but options on securities also are excluded from the definition, because the SEC already regulated such options when Dodd-Frank was enacted), instruments of indebtedness, indices, quantitative measures, or other financial or economic interests or property of any kind. The CEA contains separate provisions (which pre-date the 2010 amendments that added the swap definition) that give the CFTC separate plenary authority to regulate commodity options. The CFTC has determined to regulate most commodity options as swaps.
2. Event Contracts: This prong of the definition covers agreements, contracts or transactions for any purchase, sale, payment, or delivery (other than payment of a dividend on an equity security) that are dependent upon the occurrence,

nonoccurrence, or extent of occurrence of an event or contingency associated with a potential financial, economic, or commercial consequence. Event contracts that provide for a fixed payment based on the occurrence, non-occurrence, or extent of the occurrence of an event or contingency are also commonly referred to as binary options and may be covered by the CEA's option definition and the CFTC's separate plenary authority over commodity options.

3. Traditional Fixed vs. Floating Structures: This prong covers executory contracts for the fixed or contingent exchange of one or more payments based on the value or level of one or more underlying references[7] and that transfer between the parties, in whole or in part, the financial risk associated with a future change in any such value or level without also conveying a current or future direct or indirect ownership interest in an asset or liability that incorporates the financial risk being transferred. This part of the definition includes contracts commonly known as one of an enumerated list of contracts, such as interest rate swaps, currency swaps, agricultural swaps, or energy swaps.
4. Commonly "Known As" Structures: The definition includes a "catch-all" prong that covers contracts that are or in the future become commonly known to the trade as swaps.
5. Certain Securities-Related Swaps. The definition covers "security-based swap agreements" that meet the definition of "swap agreement" under § 206 of Gramm-Leach-Bliley Act, Pub.L. No. 106-102, 113 Stat. 133(1999), where a material term of the swap agreement is based on the price, yield, value, or volatility of any security or any group or index of securities, or any interest therein. This provision in conjunction with other statutory provisions effectively covers swaps on a broad-based index of securities as swaps that the CFTC regulates, in contrast to swaps on a narrow-based index that the SEC regulates as security-based swaps.
6. Combinations: The definition also covers any combination or permutation of the foregoing types of contracts, including any option thereon.

The statutory definition expressly excludes futures and options on futures from the swap definition. However, the category (prong #3) covering the fixed or contingent exchange of one or more payments based on the value or level of one or more underlying references also describes the cash-settlement feature of a futures contract when it is liquidated or, in the case of a cash-settled futures contract, held to expiration. Similarly, options on such a contract could be classified either as a swap or an option on a futures contract. The practical import of the exclusion is that one and the same instrument cannot simultaneously be treated as a swap and as a futures or option on a futures contract and parties should decide which classification and regulatory treatment

[7] The statutory definition specifically refers to "1 or more interest rates, other rates, currencies, commodities, securities, instruments of indebtedness, indices, quantitative measures, or other financial or economic interests or property of any kind, or any interest therein or based on the value thereof."

will apply. And as noted above, that decision could be driven by which set of regulatory requirements are best suited for the contemplated trading activity. The same overlap does not exist between the commodity option and event contract prongs of the swap definition and the definitions for futures or options on futures and transactions. Transactions covered by those parts of the swap definition are subject to the CEA's swaps regulatory regime.[8]

There is little guidance on the "commonly 'known-as'" prong of the Swap definition (Prong 4). As most readers know, the term "swap" is commonly used in crypto for all sorts of things that are not intended to refer to "Swap" in the derivative sense. Many trades are conducted on "Uniswap," for example, and many are one-for-one exchanges of assets, not "Swaps." As crypto markets develop, participants should take care with nomenclature in marketing their products; swaps regulation is one of those places where naming a thing can make it so.

The CEA regulatory regime for swaps differs in significant ways from the one for futures and options on futures. The CEA does not mandate that all swaps trading must occur on or subject to the rules of an exchange or that all trades in swaps must be cleared. The CFTC has authority, though, to designate certain types of swaps for mandatory clearing, in which case the transactions generally must be centrally cleared and may have to be executed on a CFTC-regulated trading facility, but that could be a swap execution facility ("SEF") instead of an exchange.

Importantly, to legally trade swaps away from an exchange, *i.e.*, on a SEF or bilaterally, a person must meet the definition of an eligible contract participant (ECP). This definition is more stringent than the definition of an "accredited investor" under the securities laws. Broadly, the ECP definition set out in CEA § 1a(18) and CFTC Regulation 1.3 sets high net worth/asset levels for individuals and business entities. For example, ECPs include corporations, partnerships, proprietorships, organizations, trusts, or other entities with more than $10 million in assets, as well as individuals with aggregate amounts of more than $10 million invested on a discretionary basis. Many individuals will not meet this discretionary investment test.

Regulated exchanges may list swaps for trading and some do, and the CEA permits persons that are not ECPs to trade swaps on regulated exchanges, and the exchanges are the only place where non-ECPs may legally trade swaps. All derivatives trades occurring on an exchange or subject to its rules, though, must be centrally cleared even trades in swaps that are not otherwise subject to a clearing requirement.

There are many derivative transaction types in the realm of so-called decentralized finance ("DeFi") that may be characterized as a "swap." The CFTC has brought

---

[8] A narrow exception applies with respect to commodity options, but this exception is not applicable to digital assets. The CFTC exercised its separate authority over commodity options to provide an exemption from swaps regulation for commodity options known as "trade options"; this exemption is generally available only for options on physical commodities that relate to a person's commercial operations, and which settle by delivery of the underlying commodity if exercised. See CFTC Regulation 32.3.

enforcement actions against what they described as "DeFi" protocols for illegally offering such products in the U.S. In January 2022, for example, the Division of Enforcement resolved a matter against Blockratize, Inc. d/b/a Polymarket, for offering off-exchange event-based binary options contracts, which were swaps under the CEA, and failing to obtain designation as a designated contract market (DCM) or registration as a swap execution facility (SEF).[9] Polymarket was a smart-contract based "event-based binary options online trading" platform that allowed members of the public to "bet on your beliefs" by buying and selling binary options contracts related to an event taking place in the future. In its order resolving the matter, the CFTC explained that such products were "swaps" as defined in 7 U.S.C. § 1a(47)(A)(ii), because it was an an agreement, contract, or transaction: that "provides for any purchase, sale, payment, or delivery (other than a dividend on an equity security) that is dependent on the occurrence, nonoccurrence, or the extent of the occurrence of an event or contingency associated with a potential financial, economic, or commercial consequence."

The CFTC regularly brings enforcement actions against firms and individuals illegally offering or dealing in virtual currency-related swaps. Examples include the following:

- *In re Coinflip, Inc.*, CFTC No. 15-29, 2015 WL 5535736, *1 (Sept. 17, 2015): Respondents illegally "operat[ed]a facility for the trading or processing of swaps without being registered as a swap execution facility or designated contract market." The Defendants operated a bitcoin options trading platform called Derivabit, which connected buyers and sellers of bitcoin option contracts.
- *In re Plutus Financial, Inc.*, CFTC No. 20-23 (Jul. 13, 2020): Respondents illegally entered into off-exchange swaps and operated as an unregistered futures commission merchant. Abra entered into agreements with customers (both in the U.S and overseas) whereby they would deposit Bitcoin and use it as collateral to gain price exposure on the price of another asset including foreign currencies, certain stocks and ETFs, and other cryptocurrencies.

Many have questioned whether other "DeFi" arrangements not explicitly intended to offer speculative trading arrangements are indeed swaps, including certain types of liquid staking tokens.[10]

5. Other Products Regulated by the CFTC

Other categories of transactions are regulated by the CFTC. CEA § 2(c)(2)(D) provides that agreements, contracts, or transactions in commodities (excluding foreign currencies) entered into by or offered to retail customers (non-ECPs) on a leveraged, margined or financed basis are subject to regulatory treatment "as if" they are futures,

[9] https://www.cftc.gov/PressRoom/PressReleases/8478-22
[10] *See* https://mirror.chorus.one/liquid-staking-report.pdf

subject to certain exceptions. As we discuss below, one of the exceptions covers transactions that result in "actual delivery" of the commodity within 28 days of the transaction. As covered in more detail below, the CFTC provides interpretive guidance on what constitutes "actual delivery" including guidance specific to virtual currencies, which exist in digital form.

In addition, the CEA contains special provisions in § 2(c)(2)(B) and § 2(c)(2)(C) that permit and regulate bilateral OTC trading of foreign currency futures and options on futures and leveraged transactions more generally in foreign currencies by retail customers (non-ECPs). The statutory provisions limit the persons permitted to engage in such trading with retail customers, such as retail foreign exchange dealers registered with the CFTC. The CFTC Part 5 Regulations govern retail forex activities of such persons registered with it. The CFTC has explicitly stated that these CEA provisions and CFTC regulations do not apply to trading in virtual currencies.

When faced with a product involving virtual currencies or other digital assets, it is important to "look beyond the label." Derivatives can go by labels that do not appear as defined terms in the CEA, such as "contracts for differences" ("***CFDs***") or "non-deliverable forwards" or "perpetuals." That does not mean they are unregulated under the CEA. It is important to look to the economics of a particular derivative contract, the nature or type of the underlying asset, and how the contract is traded and by whom, to determine if transactions in the contract may be subject to CEA regulation under one of the different regulatory classifications the CEA makes. CFDs, for example, could meet the swap or futures definition, or transactions in non-deliverable forwards could perhaps be subject to the CEA's provisions for leveraged retail commodity transactions.

6. Cash Market Spot and Commercial Forward Contracts – Not Regulated

As mentioned above, the CFTC generally has no authority to regulate "cash markets" for commodities. Digital assets bought or sold on a fully paid basis with immediate delivery would be characterized as cash market trading outside the CEA's reach (assuming the digital asset is not itself a derivative). Centralized exchanges (*e.g.* Coinbase) and decentralized exchanges (*e.g.* Uniswap) normally operate on such a basis, and therefore would not be regulated by the CFTC under current law so long as they do not also operate or provide markets for trading of derivatives.

"Spot contracts" traded in cash markets are contracts for the sale of a commodity for delivery where delivery occurs within two days, or such other short timeframe consistent with applicable cash market convention. The CFTC recognizes that such contracts which settle by delivery are generally outside its authority to regulate as futures or as swaps under the CEA as they lack sufficient "futurity" in the case of futures.

Similarly, certain forward contracts are excluded from regulation as futures under the CEA, pursuant to CEA § 2(a), in conjunction with § 1a(27). Section 1a(27) provides

that the term "future delivery" used in § 2(a)'s grant of jurisdiction to the CFTC over futures trading does not include "any sale of any cash commodity for deferred shipment or delivery." This exclusion has been part of the statute since its inception in 1922. Forward contracts on nonfinancial commodities (and on securities) are also excluded from the CEA's swap definition, and thus from regulation as swaps. Congress used different language to describe the exclusion than it did in the futures context, but when the CFTC and SEC jointly adopted swap product definition rules in August 2012,[11] the CFTC stated that it interprets the forward contract exclusion from both the futures and swap definitions in a consistent manner.

Broadly speaking, an excluded forward contract is a contract for the sale of a nonfinancial commodity (*e.g.*, corn or natural gas) where the parties are typically commercial in nature, defer delivery for commercial reasons, are capable of making or taking delivery and intend to make or take delivery, and where delivery routinely occurs between them. When the CFTC adopted the swap product definitions, it provided extensive interpretive guidance for determining whether contracts on nonfinancial commodities are excluded forward contracts. Forward contracts may have embedded options or options-like terms, and the interpretation addresses the types of terms that are consistent with the forward contract exclusion, to avoid classification of the contract as an option. The analysis is fact intensive, based on the specific circumstances. We are not aware of guidance that applies these principles to virtual currencies or other digital assets.

7. Allocation of Jurisdiction Between the CFTC and SEC

As noted, the CEA's commodity definition was expanded in 1974 in a manner that covers securities. This led to a period of jurisdictional disputes between the SEC and CFTC as to which agency had authority to regulate derivatives involving securities. In lieu of excluding securities from the commodity definition, Congress has amended the CEA and federal securities over the years to address areas of competing or potentially competing jurisdictional claims between the two agencies. The CFTC and SEC have also on occasion worked together to resolve jurisdictional issues. Perhaps the most important of those agreements, the Shad-Johnson Accord, was captured in statutory amendments in 1983.[12]

The bottom line is that a derivative on a digital asset that is a "security" could be subject to the CEA and the CFTC's jurisdiction, depending on the type of derivative and

---

[11] Further Definition of "Swap," "Security-Based Swap," and "Security-Based Swap Agreement"; Mixed Swaps; Security-Based Swap Agreement Recordkeeping, 77 Fed. Reg. 48208 (Aug. 13, 2012).

[12] The Futures Trading Act of 1982, enacted in January 1983, incorporated the terms of the Shad-Johnson Accord, reached between (and named after) the respective Chairmen of the SEC and CFTC as to which agency would have jurisdiction over securities-related futures and options. Futures and options on futures on individual securities (other than exempted securities) and on narrow-based indices of securities (other than exempted securities) were banned, but Congress lifted the ban in 2000.

distinctions between exempted securities and non-exempted securities and narrow-based or broad-based indices of non-exempted securities. As a general matter, SEC regulation under the federal securities laws applies to instruments that are legally classified as "securities." The term "security" as defined in § 3(a)(10) of the Securities Exchange Act of 1934 ("Exchange Act") (and in other federal securities laws) covers different types of instruments within its scope, including certain derivatives, namely, security futures products, options on a security or group or index of securities and security-based swaps.

The SEC, not the CFTC, regulates options on securities and securities indices pursuant to authority under the federal securities laws. In contrast, the CFTC, not the SEC, regulates futures and options on futures on "exempted securities" such as U.S. Treasury securities (but excluding municipal securities)[13] and on broad-based indices of other types of securities. The CFTC and SEC, though, jointly regulate futures and options on futures on individual equity securities or other securities that are not exempted securities (other than municipal securities) and on narrow-based indices of such non-exempted securities, as "security futures products."

The 2010 Dodd-Frank Act amendments added statutory provisions allocating jurisdiction between the CFTC and SEC with respect to swaps and securities-related swaps. The SEC regulates swaps based on an individual security other than an exempted security (other than a municipal security) or on a narrow-based index of such non-exempted securities as security-based swaps.[14] The CFTC regulates swaps on an exempted security (excluding municipal securities) or a broad-based index of non-exempted securities as swaps.

The classification of a digital asset (that is not itself a derivative) as a security or non-security is also important for determining which agency – the CFTC or SEC – has authority over cash market trading activities in the digital asset. As noted, the SEC – not the CFTC – regulates and has enforcement authority over cash securities markets, including enforcement authority to protect such markets against fraud and manipulation.

The following table summarizes how jurisdiction is currently allocated between the CFTC and SEC over derivatives involving securities or an interest in a security or a group or index of securities.

---

[13] "Exempted security" is defined in § 3(a)(12) of the Securities Exchange Act of 1934 and includes U.S. government securities, municipal securities, and certain other securities. It also includes foreign government debt securities enumerated in SEC Regulation 3a12-8, which the SEC has agreed to classify as exempted securities for purposes of allowing trading of futures on such foreign government debt securities.

[14] As noted above, the CEA swap definition excludes options on a security or a group or index of securities from the definition, as the SEC already regulated such options when Dodd-Frank Act was enacted. The Dodd-Frank Act amendments retained the existing provisions in the federal securities laws regulating such options, with the result that commodity options are swaps under the CEA, but securities options are not treated or regulated as security-based swaps under the federal securities laws.

Table 1: Allocation of Jurisdiction between the CFTC and SEC Over Different Types of Derivatives

CFTC	SEC	CFTC-SEC Jointly
Futures and Options on Futures		
Futures and options on futures on non-security commodities. Futures and options on futures on: A broad-based index of securities.[15] An exempted security (e.g., Treasury securities) as defined in Exchange Act section 3(a)(12). A foreign government debt security enumerated in SEC Rule 3a12-8.		Futures or options on futures on the following, regulated as "security futures products": Any security other than an exempted security or foreign government debt security enumerated in SEC Rule 3a12-8. Any narrow-based index of securities other than exempted securities. Futures on exchange-traded funds (ETFs) that passively hold non-security commodities such as gold, energy commodities, or foreign currencies are regulated as security futures, but there is an issue whether the CFTC alone should have jurisdiction over these products as futures. The CFTC issued exemptions permitting futures on commodity-based ETFs to trade as security futures products instead of treating them as futures on non-security commodities that it alone would regulate.[16]
Options on a Commodity, Security or Group or Index of Securities		
Options on non-security commodities—may be regulated as swaps or as trade options. Options on securities or a group or index of securities are excluded from the swap definition and are regulated by the SEC as securities.	Options on: Securities, without distinction between exempted or non-exempted. Any group or index of securities, without distinction between broad or narrow-based or exempted or non-exempted securities, or any	

[15] The CEA does not define the term broad-based security index, but it does define the term narrow-based security index, in CEA section 1a(35). An index is narrow-based if: (i) it has nine or fewer component securities; (ii) it has a single component security that comprises more than 30% of the index weighting; (iii) its five highest weighted component securities comprise in aggregate more than 60% of the index weighting, or (iv) its lowest weighted component securities that compromise in aggregate 25% of the index weighting have an aggregate dollar value of average daily trading volume of less than $50 million (or $30 million if the index has 15 or more component securities). The CFTC and SEC have jointly adopted rules defining the methodology for applying the statutory criteria. *See* 17 C.F.R. § § 41.11, 41.12. In addition, they have jointly adopted rules defining the criteria for an index comprised of debt securities to be classified as non-narrow, and have agreed, pursuant to joint orders, to apply alternative criteria for classifying a volatility index as non-narrow.

[16] The first was issued in 2008 and covers futures on a gold ETF that an exchange called OneChicago Exchange (which no longer exists) proposed to list. *Order exempting the trading and clearing of certain products related to SPDR® Gold Trust Shares Exemption Order*, 73 Fed. Reg. 31,981 (June 5, 2008)

CFTC	SEC	CFTC-SEC Jointly
	interest therein or based on the value thereof. Options on foreign currencies when listed on a national-securities exchange (otherwise regulated by the CFTC).[17] Options on exchange-traded funds (ETFs) that passively hold non-security commodities such as gold, energy commodities, or foreign currencies are regulated as options on securities, but there is an issue whether the CFTC has jurisdiction over such products as options based on the value of the underlying commodity. The CFTC has issued exemptions permitting such derivatives to trade on national securities exchanges, regulated as options on securities.	
Swaps / Security-Based Swaps; Including Swaptions (i.e., Options on a Swap or Security-Based Swap)		
Swaps based on a non-security commodity, including options on a non-security commodity. Swaps (other than under the CEA definition's "option" element) on: A broad-based index of securities or An exempted security (other than a municipal security) as defined in Exchange Act section 3(a)(12). Options on securities or a group or index of securities are excluded from the swap definition and are regulated by the SEC as securities. Options on the swaps described above (swaptions), including options on a (non-option variety) swap on a broad-based index of securities or an exempted security, are swaps.	Security-based swaps, *i.e.*, swaps based on: Any security other than an exempted security (other than a municipal security) or Any narrow-based securities index. Security-based swaps are generally classified as securities under the federal securities laws, but there are some differences in the regulation that applies relative to other types of securities. Because options on securities or a group or index of securities are excluded from the swap definition, they are excluded from the security-based swap definition. However, options on security-based swaps (swaptions) are generally security-based swaps.	Mixed swaps, *i.e.*, security-based swaps with a component based on the value of one or more interest rates or other rates, currencies, commodities, instruments of indebtedness, indices, quantitative measures, other financial or economic interest or property of any kind (other than a single security or narrow-based security index), or the occurrence, nonoccurrence, or the extent of occurrence of an event or contingency associated with a potential financial, economic, or commercial consequence not related to a single company or issuer.

Jurisdictional issues can still arise between the two agencies. Section 718 of the Dodd-Frank Act establishes a procedure for the CFTC and SEC to determine the status of "novel derivative products" that might implicate the regulatory interests of each agency. It allows a person filing a proposal to list or trade a novel derivative product that may have elements of both securities and futures contracts, options on futures, or commodity options to concurrently notify both agencies. In the absence thereof, if either

[17] 7 U.S.C. § 2(c)(2)(A)(iii). This provision is a bit of an anomaly. It was included in the Shad-Johnson Accord to grandfather options on foreign currencies, which were listed at the time on national securities exchanges.

agency receives a proposal to list or trade a product and determines that the proposal involves a novel derivative product that may implicate the other's jurisdiction, it must notify the other agency and provide it with a copy of the proposal. Section 718 sets out procedures and deadlines for the agencies to determine if a proposed product is within its jurisdictional remit while also specifying that one agency may challenge the other agency's determination in the U.S. Court of Appeals for the District of Columbia Circuit. The court of appeals must review the petition on an expedited basis and must not give deference to, or any presumption in favor of, either Commission's views.[18]

B. CEA Oversight Structure

1. General Overview

For anyone participating in digital assets markets, it is important to have a high-level understanding of the different types of entities and individuals involved with the derivatives markets and how they are regulated. The CEA is administered by the CFTC as an independent federal agency, which has broad authority to implement the CEA, oversee markets and market facilities and oversee industry professionals and other market participants.

The CEA establishes a framework for CFTC registration, regulation, and oversight of market facilities, *i.e.*, exchanges regulated as designated contract markets (DCMs) or as foreign boards of trade (FBOTs), organized markets for institutional swap trading called swap execution facilities (SEFs), centralized clearing houses regulated as derivatives clearing organizations (DCOs), and swap data repositories (SDRs) to which details of swaps transactions are reported. The CEA refers to DCMs, SEFs, DCOs and SDRs as "registered entities." DCMs, SEFs and DCOs are self-regulatory organizations; SDRs are not.

The CEA also establishes a separate and distinct registration and oversight regime for industry professionals. Initially, the CEA focused on registration and regulation of futures industry professionals, including futures commission merchants (FCMs), introducing brokers (IBs), commodity pool operators (CPOs) and commodity trading advisors (CTAs), and individuals acting as their associated persons (APs). Amendments to the CEA added other registration categories, including for swap dealers and major swap participants, and expanded the scope of activities that could bring a person within the definition of an FCM, IB, CPO or CTA to encompasses activities with respect to swaps. Registered industry professionals are generally referred to in the CEA and

[18] Section 718 also provides that the CFTC and SEC may request that the other agency issue an exemption with respect to a novel derivative product pursuant to their respective exemptive authorities (for the CFTC, under CEA § 4(c) and for the SEC, under Exchange Act § 36). Section 717 of Dodd-Frank amended the CEA and the Exchange Act to clarify that even if the CFTC or the SEC exempts a novel derivative product, the exempting Commission still retains jurisdiction over the product in certain cases.

various CFTC regulations as "registrants," as distinct from market facilitates as "registered entities."

The CEA relies heavily on self-regulation performed by the CFTC-regulated markets and clearing houses, and by the National Futures Association (NFA), in each case subject to CFTC oversight. Market participants are subject to varying degrees of regulation under the CEA, CFTC regulations and rules of the DCMs and SEFs, even if they are not required to register in a professional capacity under the CEA or are trading on those markets indirectly as customers.

2. The CFTC

As noted, the CFTC is an independent federal agency responsible for administering the CEA. The CEA also relies on industry self-regulation, subject to CFTC oversight. In fact, the "first line" of regulation occurs at the SRO level, with exchanges and the NFA providing the first line of defense against violations. The CFTC's functions and responsibilities over derivatives markets and their participants include the following:

1. Registration and oversight of organized markets: exchanges as designated contract markets (DCMs), foreign boards of trade (FBOTs) and swap execution facilities (SEFs).[19]
2. Registration and oversight of clearing houses as derivatives clearing organizations (DCOs).
3. Registration and oversight of registered futures associations; there is only one, the NFA
4. Registration and oversight of industry professionals.
5. Broad rulemaking authority, including in areas that can apply generally to market participants even if not registered with the CFTC. (But as noted, the CFTC's rulemaking authority generally does not extend over cash market activities.)
6. Broad enforcement authority.
7. Operation of a customer reparations program.

The CFTC conducts its mission through various divisions and offices. The largest and most important are the following:

[19] For the swaps markets, the CFTC is also responsible for registration and regulation of swap data repositories.

The Division of Clearing and Risk (DCR)

DCR oversees DCOs and other market participants in the clearing process. These include futures commission merchants, swap dealers, major swap participants, and large traders.

The Division of Enforcement (DOE)

DOE investigates and prosecutes alleged violations of the CEA and Commission regulations. Potential violations include fraud, manipulation, and other abuses concerning commodity derivatives and swaps that harm market integrity, market participants, and the general public. Within DOE is the Whistleblower Office, which administers the CFTC's whistleblower program.

The Division of Market Oversight (DMO)

DMO oversees derivatives platforms and swap data repositories. DMO reviews new applications for designated contract markets, swap execution facilities, swap data repositories, and foreign boards of trade and examines existing trading platforms and swap data repositories to ensure their compliance with the applicable core principles and other regulatory requirements, including system safeguards.

Market Participants Division (MPD)

The MPD primarily oversees derivatives market intermediaries, including commodity pool operators, commodity trading advisors, futures commission merchants, introducing brokers, retail foreign exchange dealers, swap dealers, and major swap participants, as well as designated self-regulatory organizations.

3. The NFA

NFA is a registered futures association under CEA § 17 and is an umbrella self-regulatory organization (SRO) for industry professionals required to register with the CFTC. As a general matter, the CEA requires registered industry professionals to belong to a registered futures association. (NFA is the only one.) NFA performs a role similar to the Financial Industry Regulatory Authority (known as FINRA) for the SEC-regulated securities markets and SEC-registered broker-dealers, except that NFA does not operate any market facilities. It is overseen by the CFTC and is subject to periodic compliance review.

NFA promulgates rules governing industry professionals and must enforce those rules against its members. It must submit rules and rule changes to the CFTC for review. It also processes registration applications for industry professionals (in tandem with the NFA membership process) for the CFTC pursuant to delegated authority.

NFA offers an arbitration program for handling certain types of disputes between members and their customers. It also provides a mediation program such parties may use to seek to resolve disputes between them.

4. Role of Market Facilities in Implementing the CEA Oversight Regime

Like the NFA, DCMs, SEFs and DCOs have prescribed self-regulatory responsibilities.[20] DCMs and SEFs operate market facilities for trading of derivatives. The DCMs, as exchanges, provide facilities for centralized trading of derivatives where the buying and selling interest of multiple participants interacts, typically on an anonymous basis. A SEF is also a trading platform, one on which institutional market participants (ECPs) may interact to trade swaps, under statutory provisions that promote pre-trade price transparency.

DCMs and SEFs are held to core principles under the CEA. Many of those relate to their regulatory responsibilities, including obligations to enforce compliance with their rules. They are required to submit their rules to the CFTC, either for approval or pursuant to self-certification procedures in accordance with the CFTC Part 40 Regulations. They are also required to enforce compliance with their rules against any person trading on their markets, whether that person is a member or trading indirectly through an execution intermediary. A DCM is required to provide a venue for alternative dispute resolution for market participants and market intermediaries; the statutory core principles for a SEF do not include a comparable directive.

To qualify for and maintain its registration as a DCO, a clearing house must satisfy various core principles to ensure the financial integrity of the clearing process, protect the clearing system from systemic risk, and protect the funds of clearing members and participants deposited with the DCO. The DCO's rules form a contract between the DCO and a clearing member or participant and among the DCO's clearing members or participants that define their rights and obligations to one another with respect to the clearing and settlement of derivatives transactions through the DCO. As an SRO, a DCO must have the ability to monitor compliance with its rules and to discipline a clearing member or participant for violating the DCO's rules or membership criteria. Like a DCM and SEF, a DCO must submit its rules to the CFTC under the CFTC Part 40 Regulations, either for approval or pursuant to self-certification procedures.

C. Registration and Regulation of Industry Professionals (CFTC-Registrants)

1. General Overview

The CEA sets out a registration and oversight framework for professionals operating in the futures, swaps, or retail forex markets. The registration categories include futures

[20] Although SDRs are not self-regulatory organizations, they also have a potentially important role in assisting the Commission with analysis of the swap market data reported to them for market surveillance purposes.

commission merchants (FCMs), introducing brokers (IBs), commodity trading advisors (CTAs), commodity pool operators (CPOs), swap dealers (SDs), major swap participants (MSPs), and retail foreign exchange dealers (RFED) and other categories of retail forex professionals.[21]

Individuals who act solicit customers or supervise such solicitation activities (directly or indirectly) on behalf of any of the foregoing persons (excluding SDs and MSPs) must also register with the CFTC as associated persons (APs). Individuals who are principals of a person registered in any of the foregoing categories (again excluded SDs and MSPs) are subject to fitness screening.

2. FCMs

As defined in CEA § 1a(28) and CFTC Regulation 1.3, an FCM is a person that is: (i) "engaged in soliciting or accepting orders for" certain enumerated types of derivatives, including futures and swaps; and (ii) which, in connection with those activities, accepts any money, securities or property from, or extends credit in lieu thereof to, customers, to margin, guarantee or secure the resulting trades. The definition also covers a person acting as a counterparty in leveraged retail commodity transactions.

Registered FCMs are heavily regulated, because they provide customers with access to the exchanges and clearing houses and, as clearing intermediaries, they receive and hold funds from their customers. FCMs are subject to a broad range of regulatory requirements, including:

- Minimum adjusted net capital requirements;
- Treatment, segregated holding and protection of customer funds (including obligations to contribute their own funds into the pools of customer segregated funds);
- Risk management; and
- Sales practices.

Section E below on Regulation of Custody provides more discussion of how FCMs are regulated with respect to holding protected customer funds.

3. IBs

As defined in CEA § 1a(31) and CFTC Regulation 1.3, an IB is a person that is: (i) "engaged in soliciting or accepting orders for" certain types of derivatives including futures (and swaps); but (ii) which does ***not***, in connection with those activities, accept any money, securities or property, or extend credit in lieu thereof, to margin, guarantee or secure resulting trades in such contracts.

---

[21] Along with retail forex IBs, retail forex CTAs and operators of retail forex commodity pools.

IBs are subject to minimum capital requirements and sales and trading practice requirements under CFTC regulations and NFA rules, but because they do not hold customer funds, they are not subject to customer funds segregation requirements.

4. CTAs and CPOs

As defined in CEA § 1a(12) and CFTC Regulation 1.3, a CTA is a person that, for compensation or profit, is engaged in the business of advising others on the value or advisability of trading in futures, swaps and other CFTC-regulated derivatives, *i.e.*, in "commodity interests." The primary requirements applicable to a registered CTA are set out in the CFTC Part 4 Regulations. The CFTC provides certain exemptions from registration to persons covered by the CTA definition, set out in the Part 4 Regulations.

As defined in CEA § 1a(11) and CFTC Regulation 1.3, a CPO is a person that is engaged in a business in the nature of a commodity pool or an investment trust, syndicate or other form of pooled investment vehicle that invests in futures, swaps or other commodity interests or in other pooled investment vehicles that invest in such products, and which, in connection with such business, solicits, accepts or receives funds from others through capital contributions, the sale of stock or other securities or otherwise. As a threshold matter, for a person to be a CPO, there must be a commodity pool. The primary requirements applicable to a registered CPO are set out in the CFTC Part 4 Regulations. The CFTC provides certain exemptions from registration to persons covered by the CPO definition, and certain exclusions from the CPO and commodity pool definitions, set out in the Part 4 Rules.

5. Swap Dealers and Major Swap Participants

As defined in CEA § 1a(49) and CFTC Regulation 1.3, a person is a swap dealer if it: (i) holds itself out as a dealer in swaps; (ii) makes a market in swaps; (iii) regularly enters into swaps for its own account in the ordinary course of business; or (iv) engages in activities causing the person to be commonly known as a dealer or market maker in swaps. The statutory definition excludes a person that "engages in a *de minimis* quantity of swap dealing in connection with transactions with or on behalf of its customers," as defined by the CFTC. If a person covered by the definition does not meet the *de minimis* exception, it must register with the CFTC as a swap dealer.

As defined in CEA § 1a(33), a major swap participant is a person that is not a swap dealer and whose exposures under its swap activities are so large that the person's default on its swaps positions raises systemic risk concerns,[22] as determined under prescribed exposure tests. A person that is a major swap participant is required to

[22] CEA § 1a(33) sets out three general alternative standards. The CFTC has prescribed detailed quantitative tests under the statutory elements in its definition of the term major swap participant in Regulation 1.3.

register in that capacity with the CFTC. Currently no persons are registered as major swap participants.

Swap dealers (and major swap participants, if there were any) are subject to a high degree of regulation under the CEA and CFTC regulations, primarily as set out in the Commission's Part 23 Regulations, such as minimum net capital and financial reporting requirements; requirements to collect margin from certain counterparties with respect to uncleared swaps;[23] internal and external business conduct requirements; etc. Many of those requirements can indirectly impact their end-user counterparties.

6. Retail Foreign Exchange Dealers and Other Retail Forex Professionals

A retail foreign exchange dealer (RFED) is a person that is or offers to enter into over-the-counter forex transactions of the type described in Section 2(c) of the CEA as counterparty to a retail forex customer (*i.e.*, a non-ECP), but does not include certain dealers that are permitted to trade forex opposite retail customers pursuant to the rules of the SEC or a federal banking regulator or pursuant to FCM registration. A person acting as an RFED is required to register in that capacity with the CFTC. The CEA and CFTC regulations also establishes registration categories for persons engaged in activities comparable to those of an IB, CTA or CPO for futures or swaps, but with respect to their retail forex activities. RFEDs and other retail forex professionals are subject to various requirements imposed under the CFTC Part 5 Regulations and under various NFA rules.

7. Registration of Individuals as APs and Screening of Principals

An associated person (AP) is an individual who solicits orders or customers for CFTC-regulated derivatives or, in the case of a CPO, investors in a commodity pool. The term also covers individuals who directly or indirectly supervise those solicitation activities. Individuals acting as APs for an FCM, IB, CTA, CPO, RFED, forex IB, forex CTA or forex CPO are required to register in that capacity with the CFTC and to join NFA as "associates." (The CEA contains a definition of "associated person of a swap dealer or major swap participant,"[24] but does not require individuals covered by the definition to register as APs.) An individual's registration is sponsored by the registered firm for which they will be acting as AP. An AP is subject to various CFTC regulations and NFA rules, primarily relating to sales practices.

The term "principal" is used in relation to a firm that is required to register under the CEA to identify persons that have a control-type relationship with the registrant. The "principal" definition in CFTC Regulation 3.1(a) covers individuals who, directly or

[23] If a swap dealer or major swap participant is also regulated by a federal banking regulator, the banking regulator prescribes the applicable net capital and uncleared margin requirements.
[24] CEA § 1a(4), 7 USC § 1a(4).

indirectly, exercise or can exercise a controlling influence over the activities of the firm that are subject to regulation by the CFTC, such as members of a corporation's board of director, a firm's president, chief executive officer, chief operating officer, chief financial officer, chief compliance officer or the head of a business division whose activities are subject to CFTC regulation. Principals are not required to register with the CFTC or join NFA but must undergo a fitness screening process through NFA.

D. Registration and Regulation of Market Facilities (Registered Entities)

1. Overview of Differences Between Futures Market and Swaps Markets Regulation

It is useful for legal practitioners in the digital assets space to have a basic understanding of the key differences in the CEA's approaches for regulating futures markets compared to swaps markets (which are mentioned ad hoc in prior sections). The Dodd-Frank Act amended the CEA in 2010 to impose a comprehensive regime for regulating swaps market activities, borrowing heavily from the longstanding regulation of the exchange futures markets. There are, though, fundamental differences between the two, which can be important considerations when a derivative falls in the overlap between the futures and swaps definitions described above, in deciding whether to treat the instrument as a futures contract (or option on a future) or as a swap.

Section 4(a) of the CEA requires transactions in futures contracts to occur on or subject to the rules of a board of trade designated by the Commission as a contract market, *i.e.*, as a DCM, unless exempted by the Commission. This exchange-trading requirement is read to apply to options on futures, as well. Section 4(b), though, provides that a person in the U.S. may also trade futures via "direct access" on a foreign board of traded (FBOT) that is registered with the CFTC as such. SEFs are not permitted to offer futures or options on futures for trading, only instruments classified (and regulated) as swaps. Thus, the only place where persons may legally trade futures or options on futures from locations in the U.S. is on a registered DCM or FBOT. DCMs (and registered FBOTs) may also list swaps for trading, and do not have to limit participants on their markets to eligible contract participants (ECPs).

More choices are available, but only for ECPs, on how or where they may execute a swap transaction. An ECP may execute swap transactions on a SEF or a DCM, or away from an organized market as bilateral OTC transactions unless the swap is of a type that is subject to CFTC clearing and trading mandates. A non-ECP may only legally trade swaps that are listed for trading by a CFTC-registered DCM or FBOT, and only on or subject to the rules of that listing exchange.

Clearing is another important area where differences exist. All trades in derivatives that a CFTC-regulated exchange lists for trading must be submitted to a clearing house

for clearing and settlement. Given the exchange-trading requirement for futures, trades in futures and options on futures must be cleared. In contrast, as mentioned above, the CEA does not require all trades in swaps to be centrally cleared but it does give the CFTC authority to designate certain types of swaps for mandatory clearing. For swaps subject to a clearing mandate, absent an exemption. ECPs may only execute such transactions on a SEF or a DCM if the swaps are considered "made available to trade."

As another important distinction, the feature of "cross-market fungibility" applies (to an extent) to swaps markets but not to exchange futures markets. Cross-market fungibility means that a position in a swap may be established on one market and liquidated on another. Different exchanges may offer competing futures or options on futures contracts with very similar – or even copycat – terms, but each exchange's contracts are unique to that exchange, without cross-market fungibility. In other words, if a person establishes a position in a particular futures or option on a futures contract listed by an exchange, it may only liquidate that position by establishing an offsetting position in that contract on that exchange and not with another exchange's contract.[25]

The following table recaps the main differences described above, along with some others.

Futures and Options on Futures	**Swaps**
Must be executed on or subject to the rules of an exchange; a U.S. exchange must register as a DCM. A non-U.S exchange may register as an FBOT.	Multiple trading venues for ECPs: Exchanges (DCMs or FBOTs), SEFs or bilateral/OTC. As between exchanges and SEFs, trading is more prevalent on SEFs.
Trades must be cleared by a clearing house designated by the listing-exchange; the clearing house for a DCM must be registered with the CFTC as a DCO.	Clearing is not an absolute mandate. The clearing house must be registered with the CFTC as a DCO to clear trades for U.S. persons. (In limited circumstances, the clearing house could obtain an exemption from DCO registration).
No cross-market fungibility.	Cross-market fungibility.
No trade-by-trade reporting to a trade data repository.	Reporting of individual trades to a trade data repository, referred to as a swap data repository.
No registration of dealers.	Registration of swap dealers and major swap participants.
Established framework for dealing with cross-border activities; facilitated because an exchange has an identifiable geographic locus.	Cross-border considerations more complicated to address; CEA § 2(i) generally limits CFTC jurisdiction over swaps activities outside the U.S. to those that "have a direct and significant connection with activities in, or effect on, commerce of the United States.

2. Futures Exchanges (DCMs and FBOTs)

Futures exchanges provide centralized auction markets for the contracts they list, on which trading typically occurs anonymously. Exchanges also have self-regulatory responsibilities as SROs. Exchanges surveil and police markets, looking for rule

[25] Markets participants may, though, of course establish economically offsetting positions in related contracts, including contracts listed on different exchanges, which may reduce the risk profile of their portfolio of open positions.

violations, trading irregularities, and for evidence of disruptive trading, fraud, or manipulation. When such conduct is uncovered, exchanges themselves often bring disciplinary proceedings against their market participants.

Electronic trading is the most prevalent form of centralized trading today, where orders are sent electronically to and interact on automated trade matching platforms, such as the Globex platform used by the exchanges that are part of the CME Group. An exchange may permit certain types of trades to occur away from the centralized market, pursuant to its rules.

U.S. futures exchanges must register with the CFTC as a DCM. The CEA does not provide a standalone definition of the term "designated contract market." A DCM is a type of exchange or board of trade that offers a centralized auction market for trading of the contracts that it lists where the trading interest of multiple parties interacts.

DCMs are subject to extensive regulation. A DCM must meet core principles and other requirements set out in CEA § 5, and is subject to various CFTC regulations, including the Part 38 Regulations, which prescribe more detailed obligations around complying with the statutory core principles, and oversight by the CFTC. The core principles include an obligation to provide centralized markets that are "competitive, open, and efficient" and, relating to a DCM's self-regulatory responsibilities, obligations to have market surveillance and enforcement programs and to offer arbitration programs for certain disputes relating to trading in the DCM's markets. A DCM must submit its rules and rule changes to the CFTC, in accordance with CEA § 5c(5) and the CFTC Part 40 Regulations, which include provisions that allow a DCM to submit rules with a certification that they comply with applicable CEA and CFTC requirements.

As of the date of publication, a small number of DCMs offer regulated futures or options on futures on cryptocurrency. For example, the Chicago Mercantile Exchange (CME) and Coinbase Derivatives (the d/b/a of LMX Labs, LLC) both offers futures contracts on bitcoin and on ether.[26]

U.S. participants are also permitted to trade, with some restrictions, on foreign boards of trade (FBOTs). An FBOT is a futures exchange that is located outside the U.S. If an FBOT provides "direct access" to persons located in the U.S., it must register with the CFTC as an FBOT and will be subject to various requirements under the CFTC Part 48 Regulations. "Direct access" means the exchange explicitly grants authority to persons in the U.S. to enter trades directly into the FBOT's matching system. Persons may trade futures or options on futures on an FBOT that is not registered with the CFTC, just not via "direct access."

One of the reasons why DCMs are so heavily regulated is because retail market participants are permitted to trade there, typically through an FCM. As noted, all futures and options on futures products in the U.S. must be traded on or subject to the rules of a DCM. Market participants typically must have arrangements with an FCM to

[26] For CME, *see* https://www.cmegroup.com/markets/cryptocurrencies.html and for Coinbase Derivatives *see* https://www.coinbase.com/derivatives

access a DCM's markets and the DCO that clears trades in the DCM's listed contracts. This involves establishing a futures trading account with an FCM.

Some market participants, though, clear their trades directly, without using an FCM as a clearing intermediary, by becoming clearing members of the relevant DCO (or DCOs). Although exchanges may have "members," it is generally not necessary to receive an exchange's approval as a member to trade on the exchange's market. Market participants, though, may have to meet technical, operational, or other standards imposed by the exchange or their FCM for sending orders electronically to the exchange's automated matching platform, for example if a market participant is a high frequency trading firm that generates orders automatically using computer algorithms. Some market participants may also find it advantageous to become a member of an exchange, for example to reduce the transaction fee charges imposed by the exchange or to participate in a market maker or incentive fee program offered by the exchange.

3. SEFs

The CFTC imposes different trading method requirements for swaps based on whether a swap is of a type that is subject to mandatory clearing and considered "made available to trade," or "MAT." As a general matter, if a transaction involves an interest rate swap or credit default index swap that the CFTC has designated for mandatory clearing under CFTC Regulation 50.4, parties must execute the transaction on or subject to the rules of a SEF (or a DCM), if the swap is deemed MAT on any such market. CFTC regulations refer to such transactions as "Required Transactions" and to transactions in other swaps as "Permitted Transactions." Parties may voluntarily execute Permitted Transactions on a SEF (or a DCM) but are not required to do so.

As defined in CEA § 1a(50):

> The term "swap execution facility" means a trading system or platform in which multiple participants have the ability to execute or trade swaps by accepting bids and offers made by multiple participants in the facility or system, through any means of interstate commerce, including any trading facility, that—
>
> (A) facilitates the execution of swaps between persons; and
>
> (B) is not a designated contract market.

The operator of a trading system, platform, or facility within the meaning of the CEA's SEF definition must register as such, as required under CEA § 5h, even if it limits trading to Permitted Transactions only. The use of multiple-to-multiple terminology and "accepting bids and offers" in the SEF definition implies that a system, platform, or facility must register only if it facilitates the interaction of trading interest of multiple parties on both sides of a transaction. An advisory issued by the CFTC Division of

Market Oversight (DMO) in 2021 on the SEF registration requirement,[27] though, has created some confusion as to what triggers the SEF registration requirement. The advisory suggests that one-to-one or on-to-many communication protocols could constitute multiple-to-multiple activity covered by the SEF definition, calling into question the scope of swaps brokerage activities that industry professionals may perform within the scope of their registrations (the advisory calls out IBs and CTAs) without tripping into the SEF definition.

A SEF is subject to statutory core principles set out in CEA § 5h(f), in areas such as access and trading procedures; monitoring of trading and trade processing; financial integrity of transactions; recordkeeping and reporting; antitrust considerations; conflicts of interest; financial resources; and system safeguards. A SEF must also comply with detailed requirements set out in the CFTC Part 37 Regulations on an ongoing basis.

A SEF must, at a minimum, provide an "order book" with "many-to-many" order interaction capability for both Required and Permitted Transactions. A SEF may also offer request for quote (RFQ) functionality for Required Transactions provided that the functionality meets the CFTC standard that a participant sends its RFQ to at least unaffiliated three participants; a SEF generally may not offer other methods for executing Required Transactions. In contrast, a SEF generally may offer any method for on-facility execution of Permitted Transactions, including an RFQ system with different functionality than what the CFTC prescribes for Required Transactions.

A SEF, like a DCM, is an SRO with obligations to enforce its market participants' compliance with the SEF's rules. A SEF may outsource certain enforcement oversight functions to a recognized regulatory services provider, such as NFA. As SROs, SEFs must submit rules, including rules setting out terms and conditions for the products they offer for trading, to the CFTC, either for approval or via self-certification, in accordance with the CFTC Part 40 Regulations.

Can DEXs be DCMs or SEFs or DCOs?

The growth of DeFi has led many to ask whether there is a path in the United States for U.S. users to trade or settle cryptocurrency-related derivative products via blockchain-based systems. Today, there are many DeFi protocols offering trading in products like futures, options, swaps, or what they refer to as "perpetuals" (products that behave and trade like futures contracts, but which never expire) on a peer-to-peer or peer-to-pool basis, powered by smart contracts. The details of such protocols differ, but many function similarly to regulated commodity interests and could be considered to fall within the CFTC's jurisdiction. Perhaps for this reason, many DeFi derivative protocols today operate from offshore entities and attempt to exclude U.S. customers.

[27] CFTC Letter No. 21-19, "Staff Advisory on Swap Execution Facility Registration Requirement" (Sept. 29, 2021).

Proponents of DeFi point to the fact that much of the current system of a web of regulated intermediaries (outlined in this chapter) was put in place to minimize counterparty credit risk and mutualize the risk of default. If properly programmed, smart contract systems can avoid counterparty credit risk, making defaults and failed settlements impossible with tools like overcollateralization. With the growth of DeFi, many have asked whether such DeFi derivative protocols can be offered to U.S. customers within the purview of CFTC regulation.

This leads to many questions. First, some DeFi derivatives protocols are merely collections of smart contracts living on the blockchain. Many are immutable and "ownerless." Some protocols can be adjusted and are controlled by DAOs or communities of users. It is unlikely that such entities (if "entities" is the right word to describe them) are capable of being licensed under current law and regulations.

Assuming a DeFi derivatives protocol was launched, operated, and maintained by an entity capable of being licensed, what licenses would such a product need? A DeFi derivatives protocol arguably accepts orders from retail participants, like an FCM. It arguably is a venue on which trades take place, like a DCM. Many products like perpetuals might be considered "swaps," so perhaps a SEF license is required, but the protocol would have to limit participation to ECPs, so perhaps that choice is not ideal?

Take the case of a DCM. As noted above, all DCMs must comply with the Core Principles established in section 5(d) of the CEA and Part 38 of the CFTC's Regulations. Certain of these principles seem inconsistent with a decentralized, blockchain-based system. DCM Core Principle 17 requires that the governing boards of contract markets "be designed to permit consideration of the views of market participants." How would a system of smart contracts, governed by nothing but code, meet such a principle?

A DCM must also provide centralized markets for executing transactions that are competitive, open, and efficient under DCM Core Principle 9, in compliance with prescriptive CFTC regulations as to what constitutes competitive executions and restrictions on trades that may occur non-competitively or away from the exchange's central market, which may be incompatible with the DeFi derivatives protocol.

The DCM examples highlighted above generally do not apply to a SEF under the Core Principles established in section 5h(f) of the CFTC or the CFTC's Part 37 Regulations. But other regulatory obligations do apply to a SEF that may be challenging for a DeFi derivatives protocol to meet. For example, SEF Core Principle 15 requires a SEF to designate an individual who serves as its chief compliance officer, who must have a direct reporting line to a senior officer or the board of a SEF. Clearly a protocol of smart contracts would not be able to designate a chief compliance officer.

Another challenging area: DCMs and SEFs have obligations as SROs to monitor participants' compliance with their rules and to have due process procedures in place for enforcing their rules, *i.e.*, for taking disciplinary action against a participant for

violating their rules. They are expected to have compliance and enforcement programs and staff to meet those obligations. Traditional views as to what constitutes effective self-regulation may be misaligned with how a DeFi derivatives protocol operates. Clearly a protocol of smart contracts would not be able to have such a compliance and enforcement program.

A separate question is whether a DeFi derivatives protocol may have to register as a DCO. If it is operating as a DCM, *i.e.*, it is a platform for trading futures or on which retail participants trade, then the trades must be centrally cleared. Assuming the parties to the trades settle their obligations to one another over the protocol, the protocol will likely have to register as a DCO, and the question then shifts to whether the protocol can meet the many, detailed requirements that apply to a DCO.

If DeFi derivatives protocol operates instead as a SEF for trading swaps that are not subject to a clearing mandate, then DCO registration will hinge on whether the manner in which swap trades are settled on the platform could bring the protocol within the CEA's definition of a DCO.

If DeFi derivatives protocols are to be incorporated into the CFTC's regulatory sphere, clearly the Commission would need to bend existing laws and regulations to accommodate them. Section 4(c)(1) of the CEA empowers the CFTC to "promote responsible economic or financial innovation and fair competition" by exempting any transaction or class of transactions from any of the provisions of the CEA (subject to exceptions not relevant here) where the Commission determines that the exemption would be consistent with the public interest. The Commission may grant such an exemption by rule, regulation or order, after notice and opportunity for hearing, and may do so on application of any person or on its own initiative. Section 4(c)(1) of the CEA, 7 U.S.C. 6(c)(1), provides in full:

> In order to promote responsible economic or financial innovation and fair competition, the Commission by rule, regulation, or order, after notice and opportunity for hearing, may (on its own initiative or on application of any person, including any board of trade designated or registered as a contract market or derivatives transaction execution facility for transactions for future delivery in any commodity under section 7 of this title) exempt any agreement, contract, or transaction (or class thereof) that is otherwise subject to subsection (a) of this section (including any person or class of persons offering, entering into, rendering advice or rendering other services with respect to, the agreement, contract, or transaction), either unconditionally or on stated terms or conditions or for stated periods and either retroactively or prospectively, or both, from any of the requirements of subsection (a) of this section, or from any other provision of this chapter (except subparagraphs (c)(ii) and (D) of section 2(a)(1) of this title, except that the Commission and the Securities and Exchange Commission may by rule, regulation, or order jointly exclude any agreement, contract, or transaction from section 2(a)(1)(D) of this title), if the

> Commission determines that the exemption would be consistent with the public interest.
>
> The CFTC has a long history of updating its regulations and practices to accommodate innovative technology. In one lifetime, the CFTC's markets have transitioned almost entirely from open outcry floor trading to electronic marketplaces, where high-frequency algorithmic trading is prevalent, and the CFTC worked over time to accommodate such changes in their rules. In the coming years, we look forward to proposals by responsible innovators seeking to do the same for blockchain-based systems. Such proposals could begin with limited requests for exemptive relief, and could develop over time to new rules or even statutory changes.

4. Clearing Houses

In general terms, clearing is the process by which trades in futures and options on futures or, when cleared, swaps are processed, guaranteed, and settled by a clearing house. Under a bilateral, non-cleared transaction, each party faces the risk that its counterparty may be unwilling to meet its future payment (or delivery) obligations if it has losses on the position or is unable to perform because its financial circumstances have changed. A party may address the risk of a counterparty's default through various means of credit support, such as collecting collateral from its counterparty or periodically exchanging payments covering changes in market exposure or obtaining a guarantee from the counterparty's parent. Those credit support terms are subject to negotiation between the parties and are not necessarily reciprocal.

Clearing replaces the credit support mechanisms negotiated under bilateral transactions with other mechanisms for managing counterparty default risk. When a transaction is submitted to clearing, the original trade is extinguished, and the clearing house becomes the counterparty on two replacement "back-to-back" trades through a process known as novation. By becoming inter-positioned on the trades, the clearing house then manages the default risk on a centralized basis, as a neutral third party. The clearing house manages that risk through various mechanisms, including the daily collection of margin (*i.e.*, collateral) from clearing members and daily settlement of mark-to-market gains and losses with clearing members, and required contributions by clearing members to a guarantee fund.

Market participants trading on a particular exchange must use the clearing house that the exchange designates. Parties typically access the clearing house through an FCM, which may be a clearing member of the clearing house or may act through another FCM that is a clearing member.[28] Whether the FCM provides direct or indirect access to clearing, the FCM acts as agent on behalf of its customers and guarantees its

[28] When the customer's FCM is not a clearing member, there could be more than one layer of non-clearing FCMs between the customer and the FCM clearing member, if its FCM in turn uses another non-clearing FCM, etc.

customers' performance of their obligations to the clearing house or to the clearing FCM it uses. Although the clearing house may technically become counterparty to the customer on a novated trade, the clearing house typically deals only with clearing members and not directly with the underlying customers.

When a clearing house accepts a trade for clearing, *i.e.*, at the point in time when the trade is novated, the clearing house guarantees the financial performance on the trade to its clearing members. The guarantee is not unlimited. Under certain extreme circumstances, it is possible that a loss caused by the default of a clearing member could be so large that it will have to be shared ("mutualized") across the non-defaulting clearing members. Also, the clearing house guarantee does ***not*** extend to the customers of a defaulting FCM clearing member. The purpose of the guarantee is to protect non-defaulting clearing members, and, in turn, the customers of non-defaulting FCM clearing members, against losses that may result due to another clearing member's default.

Given FCMs' integral role in the clearing process and their guarantee of their customers' performance, exchanges or their clearing houses impose requirements on FCMs to collect margin from their customers, often expressed as an initial margin requirement and a lower maintenance margin requirement. The FCM is required to collect the initial margin amount but only has to make a margin call to restore initial margin when adjustments for mark-to-market losses on positions bring the account value below the maintenance margin level. The maintenance margin levels generally equal the amount of initial margin the clearing house would require an FCM clearing member to post to it for the positions. FCMs typically require customers to deposit more margin with them than the minimum amount they are required to collect.

A clearing house must be registered with the CFTC as a DCO to clear transactions in futures or options on futures listed on a DCM. A clearing house for swaps must also register as a DCO, but a non-U.S. DCO may instead clear transactions in swaps for U.S. persons pursuant to an exemption granted by the CFTC on the basis that the non-U.S. DCO is subject to comprehensive, comparable regulation in its home jurisdiction.

As defined in CEA § 1a(15), a DCO is a clearing house or similar facility that performs any of the following functions with respect to contracts, agreements or transactions: (i) it enables the counterparties to the transactions to substitute the DCO's credit for their credit through novation or otherwise; (ii) it arranges or provides for settlement or netting of obligations, on a multilateral basis, resulting from transactions executed by participants in the DCO; or (iii) it otherwise provides clearing services or arrangements that mutualize or transfer the credit risk arising from transactions among the participants in the DCO.

DCOs are subject to extensive regulation. A DCO must meet core principles set out in CEA § 5b and other requirements set out in the CEA, and is subject to various CFTC regulations, including the Part 39 Regulations, which prescribe more detailed obligations around complying with the statutory core principles, and oversight by the

CFTC. If the Federal Stability Oversight Council[29] designates a DCO as systemically important, the DCO is subject to heightened requirements under CFTC regulations and is subject to certain oversight by the Federal Reserve Bank. (A non-designated DCO may voluntarily opt-in to the heightened CFTC requirements.) A DCO must submit its rules and rule changes to the CFTC in accordance with the CFTC Part 40 Regulations, which include provisions that allow a DCO to submit rules with a certification that they comply with applicable CEA and CFTC requirements.

5. Swap Data Repository

As defined in CEA § 1a(48), a swap data repository (SDR) is a facility that collects information and maintains records regarding transactions in swaps, including the terms and conditions of such transactions, for the purpose of providing centralized recordkeeping facilities for swaps transactions. Market participants have obligations to report their swaps transactions to an SDR under the CFTC's Part 45 Rules and with respect to real-time reporting under the CFTC Part 43 Rules. An SDR is required to register in that capacity with the CFTC and is subject to various requirements under CEA § 21 and the CFTC Part 49 Regulations. Although an SDR is not an SRO, it must submit its rules to the CFTC in accordance with the CFTC Part 40 Regulations.

E. Regulation of Custody

Custody of digital assets draws considerable attention from the industry, the financial press, Congress, and federal regulators including the CFTC, no doubt fueled by press reports of cyber-thefts, lost wallet keys, and high-profile bankruptcies such as the petition filed by FTX Trading LTD in November 2022 involving losses of digital assets held on behalf of others. Notably, though, the CEA does *not* explicitly regulate how FCMs or DCOs must hold commodities including digital assets on behalf of others on a standalone basis.

The CEA's focus with respect to custody is instead on protecting customer funds held as margin collateral for customers' cleared derivatives transactions and accruals (gains) on customers' cleared positions. In that regard, FCMs and DCOs are subject to strict customer funds segregation requirements under CFTC regulations, which implement core segregation protections laid out in the CEA. CFTC regulations establish different segregation requirements for three "account classes" of cleared derivatives: (i)

---

[29] The Federal Stability Oversight Council (FSOC) is chaired by the Secretary of the Treasury and consists of the heads of 10 federal agencies (including banking agencies, the CFTC and the SEC) as voting members, along with 5 non-voting members. Section 111 of the Dodd-Frank, which established the FSOC, grants FSOC authority to designate clearing organizations and financial market utilities as systemically important.

futures and options on futures traded on DCMs (Regulations 1.20-1.30); (ii) futures and options on futures traded on FBOTs (Regulation 30.7); and (iii) cleared swaps (Part 22 Regulations). The CFTC Part 190 Regulations governing a "commodity broker" liquidation of an FCM or DCO[30] recognizes these same account class distinctions, along with delivery accounts as a fourth account class, but FCMs and DCOs are not subject to any special custody requirements for holding property recorded in delivery accounts.

CFTC regulations define customer funds segregation requirements principally in terms of how an FCM holds customer funds and they carry that delineation forward to how segregation applies to funds that a DCO receives from an FCM clearing member. The segregation requirements imposed on FCMs reflect two interrelated policy objectives:

1. Protect the cleared derivatives markets from systemic risk, to prevent the contagion of an FCM default from spreading through the clearing system to non-defaulting clearing members and their customers. Segregation is intended to assure that an FCM has funds available to meet obligations on its customers' positions into the clearing system, as the segregated customer funds are the primary source of funds available to FCMs to meet those obligations.
2. Protect an FCM's customers in the event of the FCM's insolvency. In a bankruptcy liquidation of an FCM under the U.S. Bankruptcy Code and related CFTC Part 190 Regulations, the general principle is to distribute customer property ratably to customers by account class. If there is a shortfall in the segregated funds pool for a particular account class, the loss is shared pro rata by the FCM's customers in that account class.

At its core, segregation means that an FCM must hold its customers' funds separate and apart from its own funds, both in terms of the internal bookkeeping accounts it must maintain, and how it deposits funds with another party, *e.g.*, a bank or trust company, a DCO or another FCM. A DCO, in turn, must account for and hold customer funds it receives from an FCM separately from the DCO's own funds.

Among other restrictions, an FCM must hold segregated funds on deposit only with permissible third parties (*e.g.*, custodian banks meeting CFTC standards, another FCM or a DCO) in an aggregate amount sufficient to meet the FCM's obligations to its customers in the account class (*i.e.*, to cover the aggregate account balances of customer

[30] U.S. Bankruptcy Code contains special provisions in subchapter IV of chapter 7 governing the trustee's liquidation of a U.S. "commodity broker," including an FCM or DCO. *See* 11 U.S.C. § § 761-767. Those provisions are supplemented by CEA § 20, which authorizes the CFTC to adopt rules governing the trustee's administration of a subchapter IV proceeding. Section 20 tasks the CFTC with providing specificity to subchapter IV's general provisions. It authorizes the CFTC to determine, among other things, how the trustee should liquidate the business of the commodity broker, and the scope of what is included in or excluded from "customer property" and, for purposes of a DCO liquidation, what elements of customer property fall under the sub-classification of "member property." The CFTC adopted the Part 190 Regulations pursuant to its authority under § 20, originally in 1983. It adopted comprehensive amendments to Part 190 in December 2020.

accounts with positive balances). An FCM must also contribute its own funds into the pool of segregated funds held on deposit with third parties, to provide a cushion of excess funds and mitigate the risk of under-segregation and may not use one customer's funds to meet another person's obligations or for its own purposes (with limited exception[31]).

To the extent that bitcoin, ether, or another digital asset is an acceptable form of non-cash margin, an FCM could potentially hold the digital asset in a segregated account. In 2020, the CFTC's then Division of Swap Dealer and Intermediary Oversight (now the Market Participants Division) issued an advisory to FCMs on "Accepting Virtual Currencies from Customers into Segregation" [32] which addresses holding of virtual currencies deposited by customers to margin their futures or cleared swaps positions.[33] The advisory imposes 12 special conditions on FCMs in the form of "guidance" to address risks the Division believes that custody arrangements for digital assets present, as an overlay to the segregation requirements prescribed under CFTC regulations. The guidance is largely predicated upon an FCM's obligations under CFTC Regulation 1.11 to have risk management programs that covers segregation risks (among other risks). The conditions are largely found to be unworkable and FCMs are generally reluctant to allow customers to deposit virtual currencies into segregation.

FCMs may hold property for their customers outside of segregated accounts, in connection with cleared contracts that settle at expiration by physical delivery of the underlying commodity. The CFTC largely leaves it to the exchanges to adopt the rules governing the process for effecting deliveries under their physical delivery contracts, and to the DCOs to adopt rules setting out the obligations, if any, they assume with respect to physical deliveries (including delivery failures) under the contracts they clear. That said, in May 2023 the CFTC Division of Clearing and Risk issued an advisory on "Review of Risks Associated with Expansion of DCO Clearing of Digital Assets"[34] reminding DCOs to "actively identify new, evolving, or unique risks and implement risk mitigation measures tailored to the risks" associated with clearing of digital assets, and more generally when they expand their business lines, change business models, or offer new, novel products. The advisory highlights physical delivery of digital assets as one of several areas of heightened regulatory focus.

The CEA and CFTC regulations do not expressly permit or prohibit an FCM from facilitating deliveries in a segregated account nor do they impose any special custody requirements on an FCM when it facilitates deliveries for a customer outside a

---

[31] An FCM may invest customer segregated funds and retain the earning on such investments, but only in accordance with strict CFTC requirements that require, among other things, that the investments must be held in segregation and constitute customer property, and that the FCM must bear any losses on the investments.

[32] CFTC Letter No. 20-34 (Oct. 21, 2020).

[33] The Advisory is limited to virtual currencies that are deliverable under a physical delivery futures contract or cleared swap and does not address virtual currencies held by FCMs on behalf of customers with respect to trading on an FBOT.

[34] CFTC Letter No. 23-07 (May 30, 2023).

segregated account. In practical terms, to accomplish delivery within a segregated account, the physical delivery property must be of a type that the FCM is both willing to accept and permitted to accept under relevant exchange or DCO rules as non-cash margin that may be held in a segregated account. The advisory described above makes it highly unlikely that an FCM would allow a customer to make or take delivery of a virtual currency under a physical delivery futures or swap contract via a segregated account.

If delivery property cannot be held in a segregated account, CFTC Regulation 1.42 requires the FCM to record delivery of the commodity and the related payment in a non-segregated (*i.e.*, a non-regulated) account called a delivery account. At the bank custodian level, this means that the FCM cannot debit funds from its customer segregated bank account to pay for the delivery. (But it could transfer excess segregated funds from such a segregated bank account to its house bank account to pay for the transaction.)

F. Regulation of Leveraged Retail Commodity Trading

In addition to options, futures, and swaps, the CFTC also has jurisdiction over "retail commodity transactions" involving virtual currencies. Section 2(c)(2)(D) of the CEA, 7 U.S.C. § (c)(2)(D), provides that agreements, contracts, or transactions in commodities — other than foreign currencies or securities — entered into by or offered to retail customers (non-ECPs) on a leveraged, margined, or financed basis must be regulated as or "as if" they are futures, unless covered by an exemption. Among other things, the "as if futures," language means that covered transactions must be executed only on or subject to the rules of a CFTC-regulated exchange. Further, persons providing services in connection with covered transactions must be registered with the NFA/CFTC.

The CFTC's jurisdiction over these transactions in the context of virtual currencies was established in 2016 when the CFTC resolved an enforcement action against the international cryptocurrency exchange Bitfinex, which was offering leveraged transactions in bitcoin and other digital assets to U.S. persons without being registered as an FCM. *In re BFXNA Inc.*, Comm.Fut.L.Rep. (CCH) ¶33,766 (June 2, 2016). The CFTC has since brought cases under this authority against Kraken,[35] Ooki DAO,[36] and others.

As noted above, for these provisions to apply, the counterparty to the transaction must be "retail" (*i.e.*, not an eligible contract participant). Second, the seller must offer or execute the transaction on a leveraged or margined basis, or the transaction must be financed either directly by the seller or by a third party acting in concert with the seller. If not, then CEA § 2(c)(2)(D) is inapplicable.

---

[35] https://www.cftc.gov/PressRoom/PressReleases/8433-21.
[36] https://www.cftc.gov/PressRoom/PressReleases/8590-22

Section 2(c)(2)(D)(ii) of the CEA excepts certain transactions from Commission jurisdiction. Section 2(c)(2)(D)(ii)(III)(aa) excepts a contract of sale that results in "actual delivery" within 28 days. The purpose of the exception is to separate those transactions that actually result in the buyer obtaining the commodity from those transactions that operate like futures contract and are designed primarily for the purposes of speculation. The "actual delivery" exemption has garnered significant attention from the industry and the CFTC, which resulted in the CFTC releasing an interpretive guidance in March of 2020 (Actual Delivery Guidance). *Retail Commodity Transactions Involving Certain Digital Assets,* 85 Fed. Reg. 37,734 (June 24, 2020) (final interpretative guidance). The Actual Delivery Guidance specifies that the CFTC will employ a functional approach to the question of whether "actual delivery" occurred in such a transaction and examine how the transaction is marketed, managed, and performed, instead of relying solely on language used by the parties.

Under the Actual Delivery Guidance, actual delivery occurs in retail virtual currency transactions when:

1. A customer secures (a) possession *and* control of the entire quantity of the commodity, whether it was purchased on margin or using leverage, or any other financing arrangement, and (b) the ability to use the entire quantity of the commodity freely in commerce (away from any particular execution venue) no later than 28 days from the date of the transaction and at all times thereafter; and
2. The offeror and counterparty seller (including any of their respective affiliates or other persons acting in concert with the offeror or counterparty seller on a similar basis) do not retain *any* interest in, legal right, or control over any of the commodity purchased on margin, leverage, or other financing arrangement at the expiration of 28 days from the date of the transaction.

The Actual Delivery Guidance provides further direction on "actual delivery" of virtual currency through a number of examples. As of this writing, we are unaware of any cryptocurrency trading platform operating in reliance of the "actual delivery" exemption.

Because many arrangements in DeFi involve some aspect of leverage, margin, or financing, the prohibition against offering Retail Commodity Transactions to U.S. customers without registration is far-reaching. For example, the CFTC case that has perhaps garnered the most attention was its 2022 enforcement action against Ooki DAO. Founded by Tom Bean and Kyle Kistner, Ooki was a platform that allowed users to trade Ethereum, USDT and other cryptocurrencies on a margined or leveraged basis, in a decentralized disintermediated manner via a series of smart contracts on the Ethereum blockchain. On September 22, 2022, the CFTC issued an order (the "Order") against bZeroX LLC (the prior name for Ooki), Bean, Kistner, and the protocol's related DAO (the "Ooki DAO"), finding that the respondents violated the Commodity Exchange Act ("CEA") by unlawfully engaging in margin trading activities that could only be performed on a registered contract market and by a registered futures

commission merchant (a "FCM") under the CEA. Further, the CFTC found that the respondents failed to conduct know-your-customer diligence as required by a FCM. The CFTC also filed a related civil complaint in the Northern District of California against Ooki DAO itself.

Certain aspects of the case were controversial. Specifically, the CFTC's position – now ratified by the District Court judge in the case[37] – was that the "DAO" was an "unincorporated association" amenable to suit. But the core violation at issue was not controversial – since the 2016 *Bitfinex* case, it has been clear that persons cannot offer margined, financed, or leveraged trading in commodities like Bitcoin unless properly registered to do so. In its settlement order with the founders and their entity, the CFTC described the conduct at issue thusly:

> The bZx Protocol was a collection of smart contracts on the Ethereum blockchain that purported to facilitate transactions without intermediaries.3 The bZx Protocol enabled any person with an Ethereum wallet to contribute margin (collateral) to open leveraged positions whose value was determined by the price difference between two digital assets from the time the position was established to the time it was closed.4 For example, if a trader believed that the price of ETH would rise relative to the price of DAI, the trader might open a 5x long position in ETH versus DAI (*i.e.*, a position worth five times the increase in the price of ETH relative to DAI from the time the position was established to the time it was closed.[38]

As such, the Commission concluded, all of the elements of Section 2(c)(2)(D) were met. According to the CFTC, the DAO itself, and its founders, "entered into, executed, confirmed the execution of, and/or conducted business in the United States for the purpose of soliciting and/or accepting orders for, and/or otherwise dealing in, leveraged or margined retail commodity transactions." Retail users (*i.e.*, non-ECPs) were permitted to participate in the trading. Any product or protocol that permits users to trade or exchange digital assets on a margined, leveraged, or financed basis could fall into the same position as Ooki d*Id.*

G. The CFTC's Approach to DeFi

On September 7, 2023, the CFTC announced a trio of enforcement actions against the operators of three decentralized finance ("DeFi") protocols for offering trading in digital asset derivatives without being licensed: Opyn, Inc., Deridex, Inc., and ZeroEx, Inc.[39] In a speech the following week, the Director of Enforcement Ian McGinley discussed the

---

[37] *See* https://www.cftc.gov/PressRoom/PressReleases/8715-23.

[38] In re bZeroX, LLC et al., CFTC Docket No. 22-31 (Sept. 22, 2022).

[39] See CFTC Issues Orders Against Operators of Three DeFi Protocols for Offering Illegal Digital Asset Derivatives Trading, Release No. 8774-23, available at https://www.cftc.gov/PressRoom/PressReleases/8774-23.

CFTC's recent actions in DeFi, stating: "[t]he existence of unregulated DeFi exchanges is an obvious threat to the markets regulated and customers protected by the CFTC, and it is one we have taken very seriously."[40] These cases followed on the heels of earlier cases involving OokiDAO and Polymarket,[41] which arguably were the first to establish the CFTC's enforcement strategy concerning DeFi.

Taken together, the enforcement actions make clear that parties offering products within the CFTC's jurisdiction to U.S. customers without registration can expect an enforcement action. Take-aways from the matters include the following:

1. **DeFi not exempt.** Before the CFTC brought these matters, some developers and commentators had pushed the idea that DeFi falls outside of the CFTC's regulatory purview because the activity takes place "on chain," or in a peer-to-peer, or peer-to-pool, or via some other decentralized architecture. The recent enforcement debunked such arguments. The focus of the Commission, and of the Enforcement Division specifically, has been and will be on the nature and function of the products being traded, and whether U.S. customers had access to and participated in the activity, and not the technology used to facilitate the trading.

2. **Role of Participants.** DeFi protocols that offer derivative products often have a large and diffuse group of participants who facilitate the ultimate functionality of the protocol. This can include developers working semi-autonomously, an offshore foundation company or similar nonprofit that holds intellectual property and manages a treasury for a protocol, a group of influential users (some of whom may be the original founders), and often a U.S.-based or offshore "development company" that provides contract services to the protocol. To date, the settlements (and they have all been settlements) did not attempt to parse out the various roles being performed and consider the application of the CEA based on the role being performed.

   The three defendants in in the September 7, 2023, enforcement actions were all U.S. companies that had some significant role in developing and deploying the respective protocol. The CFTC did not consider, or even mention, other parties who had a role in governing or developing the protocol. A reasonable read of the decisions is that until challenged in court, the Division of Enforcement will take an expansive view of who may be an appropriate defendant in a similar case.

3. **U.S. Jurisdiction**. The CFTC's jurisdiction is in large part tied to the offering of jurisdictional products to U.S. persons. DeFi protocols that enable users to trade derivatives are often built directly "on chain," and anyone with an internet connection can access them. Some protocols have websites (sometimes called "front ends") that make it easier for users to access the smart contracts at issue and submit transactions. But tech-savvy users can bypass the "front end" and interact directly

[40] https://www.cftc.gov/PressRoom/SpeechesTestimony/opamcginley1.
[41] *See* https://www.cftc.gov/PressRoom/PressReleases/8478-22.

with the smart contracts. Accordingly, even if U.S.-based users could be blocked from accessing a "front end," it is difficult or impossible to conclusively exclude *all* U.S.-based users from a DeFi protocol. What does this mean for the CFTC's jurisdiction over DeFi protocols offering derivatives? Can such protocols *ever* sufficiently exclude U.S. users to avoid a CFTC enforcement action?

The September 7, 2023 *Opyn* case suggested that the answer is "maybe." In the *Opyn* case, the CFTC found Opyn liable for failure to register even though it "took certain steps to exclude U.S. persons from accessing the Opyn Protocol, such as blocking users with U.S. internet protocol addresses," because "those steps were not sufficient to actually block U.S. users from accessing the Opyn Protocol," possibly because U.S. traders were accessing Opyn via VPN or directly to the smart contracts (the order does not say). In resolving the case, CFTC staff credited Opyn for taking "additional steps to block U.S. users' access to the Opyn Protocol." Ultimately, Opyn paid a fine but did not shut down. This resolution suggests, but does not explicitly state, that the Commission believes there are steps protocols can take to sufficiently block U.S. users that the CFTC is comfortable with. What were the steps Opyn took to satisfy the CFTC? The question is left unanswered.

Many if not most centralized exchanges perform KYC on their users, which is the "gold standard" in terms of excluding U.S. participants. As part of its 2023 settlement with the CFTC, Binance implemented a detailed and comprehensive procedure laying out how it will conduct such diligence on individuals and entities with U.S. connections.[42] Implementing such a procedure requires a huge investment in staff, training, and processes. Few in the "DeFi" space currently follow such a strategy.

Instead, some "DeFi" protocols implement front-end controls such as: (1) stating in terms of service that U.S. participants are prohibited; (2) implementing restrictions on IP addresses to block users attempting to access the front end from the United States (called "geofencing"); (3) attempting to block or restrict VPN usage so that traders in the United States cannot avoid such restrictions; and (4) implementing other technology designed to identify and exclude U.S. users. It is likely that Opyn did some combination of this, but the CFTC has not announced it.

In addition, the CFTC's enforcement actions against both Opyn and ZeroEx referenced the fact that Section 4(a) of the CEA, 7 U.S.C. § 6(a), makes it illegal to "conduct[] an office or business in the United States" for the purpose of soliciting or accepting orders for, or otherwise dealing in off-exchange futures or retail commodity transactions with non-ECPs. This provision is relevant to individuals and teams working within the U.S. to offer these protocols. To date, the Enforcement

[42] See https://www.binance.com/en/about-legal/assessment-of-us-connections.

Division has not relied *exclusively* on this provision as the basis for its jurisdiction; each case has included U.S. users utilizing the products at issue.

4. **"Facilitation" of Access to Derivatives.** The ZeroEx matter stands for the proposition that, at least according to this one settlement, the CFTC can sue a protocol for "facilitating" access to derivatives trading, even if that protocol had no involvement in developing or deploying the product at issue. In ZeroEx, the CFTC took issue with the fact that some unknown third party had used the ZeroEx swap protocol to list certain "Leveraged Tokens," which the CFTC found embodied retail commodity transactions as discussed above. ZeroEx itself did not develop or list the Leveraged Tokens.

   Section 2(c)(2)(D) of the CEA provides that the section applies to any "agreement contract, or transaction" with a non-ECP that is entered into or offered on a leveraged, margined or financed basis "by the offeror, the counterparty, ***or a person acting in concert*** with the offeror or counterparty on a similar basis." (emphasis added). There has been very little precedent or caselaw interpreting what "acting in concert" means in the context of Section 2(c)(2)(D) Probably the best source of authority is the CFTC's 2020 guidance on "actual delivery."[43] In that guidance, the Commission noted that it would interpret the phrase "offeror" broadly "to encompass any persons that present, solicit, or otherwise facilitate a retail commodity transaction under the Act" and could include "those with operational control of a particular blockchain protocol." *Id.* at FN 164. The guidance also recognized that even an unaffiliated third-party could be acting "in concert" with an offeror if they provide financing or leverage to an end user. *See Id.* at 165.

   In the ZeroEx settlement, the CFTC did *not* conclude that the defendant was "acting in concert" with the unknown and unaffiliated third parties who developed and issued the "Leveraged Tokens." Instead, even though Section 2(c)(2)(D) does not use the word "facilitate," the CFTC essentially read that word into the statute. As such, as explained in footnote 8 of the ZeroEx order, the basis on which the CFTC held the defendant responsible for the trading of the Leveraged Tokens was through their "facilitation" of access to margin or leverage. Specifically, it was enough for ZeroEx to have deployed and operated technology that "'facilitated' and 'provide[d] a purchaser with the ability to source financing or leverage from other users or third parties." This resolution is another example of an expansive and aggressive interpretation, signaling that the CFTC could attempt to sue players in the DeFi space that do not themselves offer trading in jurisdictional products, but support or facilitate it.

[43] https://www.cftc.gov/sites/default/files/2020/06/2020-11827a.pdf.

Bank Secrecy Act and Web3

Anti-Money Laundering and Countering the Financing of Terrorism (AML/CFT) Regulatory and Enforcement Regimes

Logan Payne, Kate Roin, and Sarah Shtylman*

A. Introduction

Through the Bank Secrecy Act ("BSA"), the United States maintains a multifaceted policy regime for tackling anti-money laundering ("AML"), combating the financing of terrorism ("CFT"), and countering illicit financial threats. This Chapter provides an overview of the U.S. government's AML/CFT regulatory and enforcement regimes for Web3.

B. The BSA Regime

In the 1950s and 1960s, members of Congress expressed concern over the use and abuse of cash deposits, foreign bank accounts, and other mechanisms to "launder" proceeds from illegal operations, evade taxes, and facilitate the conduct of illegal activity.[1] Money laundering broadly refers to the process of disguising financial assets so they can be used without revealing their underlying illicit source or nature (e.g., proceeds of fraud, corruption, and contraband trafficking). In 1970, these concerns led to the enactment of what is now known as the BSA.[2]

The purpose of the BSA was to help identify the source, volume and movement of currency and other monetary instruments transported or transmitted into or out of the

---

* Payne is Counsel at Perkins Coie in Austin, TX (https://www.perkinscoie.com/en/professionals/logan-s-payne.html), Roin is a Partner at BarlitBeck in Chicago, IL (https://www.bartlit-beck.com/lawyers-KatharineRoin); and Sarah Shtylman is a Partner at Perkin Coie in Palo Alto, CA (https://www.perkinscoie.com/en/professionals/sarah-shtylman.html). Olta Andoni, General Counsel at Enclave Markets, reviewed this chapter.

[1] The policy goals are discussed at length in the BSA's legislative history. *See generally* S. Rep. No. 91-1139 (1970); H.R. Rep. No.91-975 (1970).

[2] The BSA, as amended, is codified at 12 U.S.C. § 1829b, 12 U.S.C. § § 1951-1960, 31 U.S.C. § § 5311-5314, 5316-5336.

United States, which Congress found had a "high degree of usefulness in criminal, tax, or regulatory investigations or proceedings."[3] The law was a means of combating the use of "secret foreign bank accounts and foreign financial institutions as part of illegal schemes by American Citizens and others. . . ."[4]

Over the following five-plus decades, Congress amended the BSA and related provisions to address other illicit financial threats, including proliferation finance, tax evasion, sanctions evasion, terrorist financing, and the financial facilitation of other state and nonstate threat actors. As amended, the BSA comprises over a dozen separate legislative acts.

1. Foundation: 1970-1984

In 1970, Congress enacted the BSA, formally enacted as the Bank Records and Foreign Transaction Act.[5] Title I required banks and other financial institutions to record and retain certain financial records for periods of up to five years.[6] Because the "effective fight on crime depends in large measure on the maintenance of adequate and appropriate records by financial institutions, [Title I] deals with the problem by requiring the maintenance of records by financial institutions in a manner designed to facilitate criminal, tax and regulatory investigations and proceedings."[7] Title II required banks and other financial institutions and, in some instances, individuals, to report to the government certain transactions that are of particular interest to regulatory and law enforcement agencies because "such reports have a high degree of usefulness in criminal, tax, or regulatory investigations or proceedings."[8]

The original 1970 legislation authorized the Secretary of the Treasury (the "Secretary") to issue regulations requiring various reports and recordkeeping of insured and uninsured financial institutions and individuals.

In addition, the legislation provided for civil and criminal penalties, primarily at the level of $1,000. Many of the statutory requirements are still in effect (as amended) over fifty years later.[9]

---

[3] 12 U.S.C. § § 1829b(a)(2) (1970); Courtney J. Linn, Redefining the Bank Secrecy Act: Currency Reporting and the Crime of Structuring, 50 Santa Clara L. Rev. 407 (2010).

[4] Hearings on H.R. 15073 Before the House Committee on Banking and Currency, 91st Cong., 1st and 2d Sess., 8 (1970); L. Gene Sanford, California Bankers Association v. Shultz: An Attack on the Bank Secrecy Act, 2 Hastings Const. L.Q. 203 (1975).

[5] Pub. L. No. 91-508, 84 Stat. 1114 (1970). The first two titles of this legislation are entitled: "I. Financial Recordkeeping" and "II. Currency and Foreign Transactions Reporting Act." Titles I and II, collectively, were referred to informally as the Bank Secrecy Act.

[6] *See* 12 U.S.C. § § 1829b, 1951-1959.

[7] H.R. Rep. No. 91-975, at 10 (1970).

[8] *See* 31 U.S.C. § § 5311-5322. Title II was codified at 31 U.S.C. § § 1051-1122. In 1982, these sections were re-enacted without substantive change as 31 U.S.C. § § 5311 to 5322 and retitled Records and Reports on Monetary Instruments Transactions.

[9] As of 2022, financial institutions must file a Currency Transaction Report (CTR) for any transaction that exceeds a momentary threshold of $10,000.

The BSA has been challenged on several occasions throughout its history, particularly in the years after its enactment, and with few exceptions has survived. For example, In 1974, in *California Bankers Association v. Shultz*, the U.S. Supreme Court upheld the constitutionality of the recordkeeping and reporting provisions of the BSA against First, Fourth, and Fifth Amendment attacks.[10] There, the Supreme Court found that the BSA (1) did not violate the due process clause by placing unreasonably burdens on the banks; (2) did not violate the Fourth Amendment because the mere maintenance of records by banks was not a seizure, and (3) that the first amendment challenge by the ACLU was premature and there was no justiciable case or controversy since the ACLU had not shown any proof that the government attempted to compel the production of records.[11] As to the second issue, whether or not there was a seizure, the Court found only that there had not yet been a seizure at the banks record keeping phase because the government had not yet acquired the records from the bank.[12] The Court's decision left the question of seizure undecided. But not for long.

Just two years later, in 1976, the Supreme Court heard its second case challenging the BSA. In *United States v. Miller*, 425 U.S. 435, 442–43 (1976), a man named Mitch Miller challenged the government's access to his bank records. Miller was indicted for various federal offenses related to his operation of a still, and he made a pretrial motion to suppress copies of checks, deposit slips and other records from two banks, which had maintained the records pursuant to the BSA.[13] Miller argued that the subpoena pursuant to which the banks had produced his bank records was an illegal seizure in violation of the Fourth Amendment. Specifically, Miller argued that he had a Fourth Amendment interest in the records kept by the banks because they were copies of personal records made available to the banks for a limited purpose and in which he had a reasonable expectation of privacy.[14]

The Supreme Court disagreed, stating "[t]he lack of any legitimate expectation of privacy concerning the information kept in bank records was assumed by Congress in enacting the Bank Secrecy Act, the expressed purpose of which is to require records to be maintained because they 'have a high degree of usefulness in criminal tax, and regulatory investigations and proceedings.'"[15] "[T]he Fourth Amendment does not prohibit the obtaining of information revealed to a third party and conveyed by him to Government authorities, even if the information is revealed on the assumption that it will be used only for a limited purpose and the confidence placed in the third party will not be betrayed."[16] Under *Miller*, the banks had "no legal obligation to notify the

---

[10] California Bankers Ass'n v. Shultz, 416 U.S. 21, 24, 94 S. Ct. 1494, 1500, 39 L. Ed. 2d 812 (1974).
[11] *Id.*
[12] Nancy M. Kirschner, The Right to Financial Privacy Act of 1978-The Congressional Response to United States v. Miller: A Procedural Right to Challenge Government Access to Financial Records, 13 U. Mich. J.L. Reform 10, 18 (1979).
[13] *U.S. v. Miller*, 425 U.S. 435 (1976).
[14] *Id.* at 442.
[15] *Id.* at 442-443 (citing 12 U.S.C. § 1829b(a)(1)).
[16] *Id.* at 443.

customer of the government's request for information, and, even if Miller had been notified, he would not have had standing to contest their production" to the government.[17]

In response to *Miller*, there was a wave of federal and state financial privacy legislation.[18] In 1978 Congress enacted the Right to Financial Privacy Act, which gave individuals and partnerships the right to contest the disclosure of banking records to the government on the basis that they are not relevant to a legitimate law enforcement inquiry.[19] But instead of creating a substantive and legally enforceable right to financial privacy in response to the BSA, the Right to Financial Privacy Act merely enumerated procedural safeguards that the government had to follow in order to access financial information.[20]

2. Evolution: 1984-2001

In the 1980s and 1990s, Congress amended the BSA several times to expand the policy tools available to combat organized crime, drug trafficking, and more modern methods of attempted money laundering.

In 1970, when Congress first enacted the BSA, it was generally understood that the penalty thresholds – many of which were set at $1,000 – were comparatively modest but were nevertheless thought to be an effective deterrent. In 1984, leveraging over a decade of experience of BSA implementation, Congress determined that an increase in the penalties was needed to enhance the deterrence effect of the BSA. Congress passed the Comprehensive Crime Control Act of 1984, which stiffened the criminal and civil penalties for violations.[21]

As originally enacted, the BSA did not authorize the government to prosecute money launderers for "structuring," a money laundering technique that involves breaking down large amounts of funds into multiple smaller amounts, and depositing those funds into many different accounts to avoid detection and circumvent recordkeeping and reporting thresholds. In 1986, Congress passed the Money Laundering Control Act of 1986, which prohibited structuring transactions to evade currency transaction reporting filings and established certain criminal penalties for money laundering.[22]

In 1988, Congress enhanced the BSA again with the Money Laundering Prosecution Improvements Act, which strengthened certain verification requirements.[23]

---

[17] Kirschner, supra n. 12.
[18] See James E. Eldridge, The Bank Secrecy Act: Privacy, Comity, and the Politics of Contraband, 11 N.C. J. Int'l L. 667, 680 (1986).
[19] *See* 12 U.S.C. § 3301 et seq.
[20] *Id.*
[21] Pub. L. No. 98-473.
[22] Pub. L. No. 99-570. *See* 18 U.S.C. § 1956 (laundering of monetary instruments); *Id.* § 1957 (engaging in monetary transactions in property derived from specified unlawful activity).
[23] Pub. L. No. 100-690, Title VI, Subtitle E.

A more substantial enhancement of the BSA took place in 1992 with the enactment of the Annunzio-Wylie Anti-Money Laundering Act, which introduced many critical provisions that are still prominent today, including the prohibition on illegal money transmitting businesses, know-your-customer ("KYC") rules, and the requirement that any financial institution, and any director, officer, employee or agent of a financial institution file suspicious activity reports ("SARs") for any transaction of at least $5,000 that they know, or have reason to know, or reason to suspect are derived from illegal activity, or those that they believe are designed to "hide or disguise funds or assets derived from illegal activities."[24] With the additional requirements and penalties, the Annunzio-Wylie Anti-Money Laundering Act increased the risks to financial institutions of any involvement in money laundering, but also provided some protection for compliance with the reporting requirements.[25]

In 1994, the Money Laundering Suppression Act introduced a registration requirement for money services businesses ("MSBs").[26] It overturned a decision in a then-recent Supreme Court case, *Ratzlaf v. United States*, by eliminating the willfulness requirement for certain BSA violations.[27]

In 1998, the Money Laundering and Financial Crimes Strategy Act, required the Treasury Department to develop and implement a national strategy to combat money laundering and related financial crimes. It also authorized the Treasury Department to designate geographic areas as high-risk for money laundering and related financial crimes, making such areas eligible for targeted law enforcement action.[28]

3. USA PATRIOT Act: 2001-2020

Shortly after the September 11, 2001, terrorist attacks, Congress enacted the Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act ("USA PATRIOT Act").[29] Title III of the USA PATRIOT Act, the Money Laundering Abatement and Financial Antiterrorism Act of 2001, strengthened the BSA's existing anti-money laundering tools and added new tools to combat the

---

[24] Pub. L. No. 102-55; 31 U.S.C. § 5318(g)(1) at 4331-4332. The statutory requirement for SARs is codified at 31 U.S.C. § 5318(g).

[25] See Duncan E. Alford, Anti-Money Laundering Regulations: A Burden on Financial Institutions, 19 N.C. J. Int'l L. 437, 464 (1993).

[26] Pub. L. No. 103-325.

[27] In Ratzlaf v. United States, 114 S. Ct. 655 (1994), the Court attempted to resolve the question of whether the government must prove that the defendant knew that structuring was unlawful to convict the person for "willfully" violating the BSA. A provision of the MLSA modified the BSA to deny a defendant the opportunity of an "ignorance of the law" defense in structuring cases, effectively overruling the Court's decision in Ratzlaf. *See* H.R. Rep. No. 438, 103d Cong. (1994) ("This section makes clear that violation of the prohibition on structuring transactions to evade currency reporting, 31 U.S.C. § 5324, requires only an intent to evade reporting requirements, not proof that the defendant knew that structuring was illegal.")

[28] Pub. L. No. 105-310.

[29] Pub. L. No. 107-56.

financing of terrorism, turning the BSA from an AML framework into an AML/CFT framework.

Title III of the USA PATRIOT Act, like other legislation that has amended the BSA, has been codified into statute and implemented through the BSA Regulations, but the substantive provisions are still commonly described by reference to their place in the original text of the legislation:

> Section 311 authorized the Secretary of the Treasury to take certain "special measures" against foreign jurisdictions, banks, accounts, or transactions found to be of primary money laundering concern.[30]
>
> Section 312 requires certain due diligence and enhanced due diligence with regard to foreign correspondent accounts and large private banking accounts provided to non-U.S. persons.[31]
>
> Section 313 prohibits the establishment or maintenance of correspondent accounts for a foreign shell bank and required reasonable steps to be taken to ensure that other foreign correspondent accounts are not used indirectly by shell banks.[32]
>
> Section 314 authorized the Secretary to promulgate regulations for the sharing of information between the government and financial institutions and between financial institutions.[33]
>
> Section 352 requires financial institutions to implement written anti-money laundering programs ("AML Programs").[34] The AML Program is a cornerstone of the modern AML/CFT framework.

4. Anti-Money Laundering Act: 2020-Present

On January 1, 2021, Congress passed the National Defense Authorization Act for Fiscal Year 2021 ("2021 NDAA").[35] "Division F" of the 2021 NDAA encompassed several anti-money laundering provisions known collectively as the Anti-Money Laundering Act of 2020 ("AMLA"). AMLA made meaningful changes to the BSA for the first time since the USA PATRIOT Act of 2001.

---

[30] *See* 31 C.F.R. § § 1010.651 to 1010.670.
[31] *See* 31 C.F.R. § § 1010.605 to 1010.620.
[32] *See* 31 C.F.R. § § 1010.605, 1010.630.
[33] *See* 31 C.F.R. § § 1010.500 to 1010.540.
[34] Since 1987, all federally insured depository institutions and credit unions have been required by their federal regulators to implement anti-money laundering programs "to assure and monitor compliance with the requirements" of the BSA, but until the passage of the USA PATRIOT Act in 2001, the requirement to implement such programs did not arise under a specific provision of the BSA itself. The scope of the requirement has since been expanded to all "financial institutions" as defined under the BSA.
[35] Pub. L. No. 116-283.

AMLA provides U.S. law enforcement with several potentially powerful tools for combating money laundering. Within AMLA is the Corporate Transparency Act, which for the first time imposed a federal requirement for identifying beneficial owners of certain legal entities (*i.e.*, the natural persons who own or control, directly or indirectly, such entities). AMLA also authorized the application of additional civil penalties for repeat BSA violators,[36] barred certain BSA violators from serving on boards of U.S. financial institutions,[37] and added a new prohibition on the concealment of the source of assets in monetary transactions.[38]

As relevant to Web3, AMLA also expanded the scope of the BSA statute to cover certain businesses that provide services involving "value that substitutes for currency." AMLA amended the definition of "financial institution" to make it clear that currency exchanges and money transmitting businesses covered by the BSA include businesses that provide services involving "value that substitutes for currency,"[39] which includes certain types of digital assets.

5. Office of Foreign Assets Control Sanctions

The Office of Foreign Assets Control ("OFAC") is an office of the Treasury Department that administers and enforces economic and trade sanctions based on U.S. foreign policy and national security goals against targeted individuals and entities.

OFAC sanctions are separate and distinct from the BSA, but because they share the common goal of preventing illicit financial activity, compliance with OFAC sanctions is frequently assessed alongside compliance with the BSA. Notably, compliance with OFAC sanctions is required of all U.S. persons (including businesses), regardless of whether the person is engaged in providing financial services.

OFAC sanctions compliance obligations are the same regardless of whether a transaction is denominated in digital assets or traditional fiat currency.[40]

Because each sanctions program is based on different foreign policy and national security goals, prohibitions may vary between programs. When programs prohibit transactions with targets, U.S. persons may not engage in trade or financial transactions and other dealings with the target unless authorized by OFAC or expressly exempted by statute. OFAC may also order U.S. persons to "block," or freeze, property of a sanctioned target. When property is "blocked," title to the property remains with the target, but the exercise of powers and privileges normally associated with ownership is prohibited without authorization from OFAC. Blocking immediately imposes an across-

---

[36] AMLA § 6309.
[37] AMLA § 6310.
[38] AMLA § 6313.
[39] *See* AMLA § 6102(d) (amending 31 U.S.C. § 5312(a)(2)).
[40] OFAC, "Frequently Asked Questions No. 560" (Mar. 19, 2018), https://ofac.treasury.gov/faqs/560#:~:text=Yes%2C%20the%20obligations%20are%20the%20same.%20U.S.%20persons,in%20trade%20or%20other%20transactions%20with%20such%20persons.

the-board prohibition against transfers or dealings of any kind with regard to the property.

OFAC sanctions violations carry strict liability, and the fines for sanctions violations can be substantial – in many cases, civil and criminal penalties have exceeded several million dollars. While not required by any specific regulation, a best practice for all U.S. persons is to establish and maintain an effective, written OFAC compliance program ("OFAC Sanctions Compliance Program") that is commensurate with the person's OFAC risk profile (based on products, services, customers, and geographic locations).

In 2019, OFAC published its *Framework for OFAC Compliance Commitments* ("OFAC Compliance Framework") which provides detail on the five essential components of an OFAC Sanctions Compliance Program: management commitment, risk assessment, internal controls, testing/auditing, and training.[41]

In 2021, OFAC issued compliance guidance that builds on the OFAC Compliance Framework and provides additional detail specifically tailored to the virtual currency industry (the "OFAC Virtual Currency Guidance").[42] The OFAC Virtual Currency Guidance provides an overview of OFAC sanctions requirements and procedures, licensing and enforcement processes, and compliance best practices tailored for digital assets. The OFAC Virtual Currency Guidance uses recent OFAC enforcement actions as "case studies" to illustrate these principles in action.

Recent OFAC enforcement actions against digital asset companies emphasize the importance of ensuring that companies implement controls to screen location-related information collected during the normal course of address information, such as billing addresses, IP addresses, and email address suffixes.[43]

C. Web3 Businesses as "Financial Institutions"

Under the BSA, the definition of "financial institution" determines the scope of applicability of the BSA's requirements and obligations.[44]

The BSA imposes such obligations on a wide range of financial institutions.[45] Determining whether an entity, including an entity engaged in the Web3 ecosystem, is a

---

[41] *See generally* OFAC, "A Framework for OFAC Compliance Commitments" (May 2, 2019) ("OFAC Compliance Framework").

[42] OFAC, "Sanctions Compliance Guidance for the Virtual Currency Industry" (Oct. 15, 2021) ("OFAC Virtual Currency Guidance").

[43] *See, e.g.*, OFAC Enforcement Release, "OFAC Enters Into $98,830 Settlement with BitGo, Inc. for Apparent Violations of Multiple Sanctions Programs Related to Digital Currency Transactions" (Dec. 30, 2020); OFAC Enforcement Release, "OFAC Enters into $507,375 Settlement with BitPay, Inc. for Apparent Violations of Multiple Sanctions Programs Related to Digital Currency Transactions" (Feb. 18, 2021).

[44] *See* 31 U.S.C. § 5312(a)(2).

[45] 31 C.F.R. § 1010.100(t)(1)-(10). These categories are: a bank (except a bank credit card system); a broker or dealer in securities; a money services business; a telegraph company; a casino; a card club; a person subject to supervision by any state or Federal bank supervisory authority; a futures commission merchant; an introducing broker in commodities; and/or a mutual fund.

covered financial institution will depend on specific facts and circumstances surrounding its financial activities.

1. Financial Institutions Subject to Other Regulatory Frameworks

The majority of financial institutions covered by the BSA are defined as such as because they are subject to other U.S. financial regulatory frameworks. Futures commission merchants and introducing brokers are obligated to register with the Commodity Futures Trading Commission ("CFTC"); broker-dealers and mutual funds are obligated to register with the Securities and Exchange Commission ("SEC"); and banks and other institution types chartered under banking laws are supervised by a federal or state banking authority.

The nature of the activities in which a person engages is the key factor in determining whether and how that person must register with, or obtain regulatory approvals from, the CFTC, SEC, or banking authorities. These regulators rigorously enforce these requirements and have taken numerous actions against Web 3 entities that have failed to comply, many of which have also involved charges that the entity did not implement an adequate BSA AML Program as required.

2. Financial Institutions Not Subject to Other Regulatory Frameworks

Although a large part of the Web3-related financial ecosystem in the U.S. is covered by the regulatory structure discussed above, some business models still fall outside it. Unless and until there is action by policymakers to add new digital asset-specific categories of "financial institution" to the BSA or otherwise,[46] and assuming that a Web3 entity is not subject to the regulatory frameworks of the CFTC, SEC, or banking

[46] Policymakers have proposed, but not yet enacted, amendments to the BSA's definition of "financial institution" to expressly cover more digital asset-related activities. For example, citing the warnings from the "Treasury Department, Department of Justice, the Federal Bureau of Investigation, and other national security and law enforcement experts" that "digital assets are increasingly being used for money laundering, ransomware attacks, theft and fraud schemes, trafficking, terrorist financing, and other crimes," the Digital Asset Anti-Money Laundering Act of 2023 proposes to create a new category of "financial institution" under the BSA to cover "unhosted wallet providers, digital asset miners, validators, or other nodes that may act to validate or secure third-party transactions, independent network participants (including maximal extractable value searchers), miner extractable value searchers, other validators or network participants with control over network protocols, or any other person facilitating or providing services related to the exchange, sale, custody, or lending of digital assets that the Secretary shall prescribe by regulation." (Digital Asset Anti-Money Laundering Act of 2023, S. 2269, 118th Cong. (2023); Sen. Elizabeth Warren and Sen. Roger Marshall, "The Digital Asset Anti-Money Laundering Act of 2023" (July 26, 2023).) A competing bill, the Crypto-Asset National Security Enhancement and Enforcement Act of 2023, also proposes to create a new category of "financial institution" under the BSA but would define it to cover any "digital asset transaction facilitator or a digital asset protocol backer." (Crypto-Asset National Security Enhancement and Enforcement Act of 2023, S. 2355, 118th Cong. (2023).)

regulators, the category of "financial institution" under the BSA that is most likely to apply to a Web3 entity engaged in activities of a financial nature is that of "money services business" ("MSB").[47]

3. Web3 Businesses as "Money Services Businesses"

The BSA Regulations divide the category of "MSB" into seven sub-categories: foreign exchange dealer; check casher; issuer of traveler's checks or money orders; provider of prepaid access; money transmitter; the U.S. Postal Service; and seller of prepaid access.[48] Persons doing business in the capacity of any of these sub-categories are "financial institutions" (specifically, MSBs) under the BSA.

For Web3 entities engaged in activities of a financial nature, the sub-category of "money transmitter" is most relevant. A "money transmitter" is defined as a person that provides money transmission services, or any other person engaged in the transfer of funds. The term "money transmission services" is defined as "the acceptance of currency, funds, *or other value that substitutes for currency* from one person and the transmission of currency, funds, *or other value that substitutes for currency* to another location or person by any means" (emphasis added).[49]

Whether a person is a money transmitter is a matter of facts and circumstances,[50] and on March 18, 2013, FinCEN released guidance (the "FinCEN 2013 CVC Guidance") taking the position that "exchangers" and "administrators" of digital assets with specific characteristics — "convertible virtual currency" or "CVC" — are money transmitters.[51] CVC is "value that substitutes for currency," and because the actions of "exchangers" and "administrators" constitute transmission (as each is described in the FinCEN 2013 CVC Guidance), such participants in Web3 ecosystems are money transmitters under the BSA. The FinCEN 2013 CVC Guidance distinguished "exchangers" and "administrators" from "users" — persons who obtain CVC for their own personal use, such as to purchase goods and services — and concluded that the activity of a "user," as described in the FinCEN 2013 CVC Guidance, does not constitute "money transmission

---

[47] Web3 entities engaging in activities of a "card club," "casino," or "telegraph operator" may be "financial institutions" under the BSA. *See* 31 C.F.R. § 1010.100(t). The discussion in this Chapter focuses on Web3 entities engaged in activities of a financial nature.

[48] 31 C.F.R. § 1010.100(ff).

[49] 31 C.F.R. § 1010.100(ff)(5)(i)(A).

[50] 31 C.F.R. § 1010.100(ff)(5)(ii).

[51] *See* FinCEN, FIN-2013-G0001, "Application of FinCEN's Regulations to Persons Administering, Exchanging, or Using Virtual Currencies" (Mar. 18, 2013). Specifically, the FinCEN 2013 CVC Guidance defines an exchanger as a person or entity "engaged as a business in the exchange of virtual currency for real currency, funds, or other virtual currency." The FinCEN 2013 CVC Guidance also defines an administrator of virtual currency as a person or entity "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."

services" and therefore is not subject to FinCEN's registration, reporting, and recordkeeping regulations for MSBs.[52]

FinCEN described "CVC" as inclusive of digital assets that are not legal tender but have an equivalent value in, or act as a substitute for, "real currency" (*i.e.*, government-issued legal tender currency).[53] In May 2019, in updated and more detailed guidance (the "FinCEN 2019 CVC Guidance"), FinCEN reiterated and elaborated on this point, explaining that "other value that substitutes for currency" encompasses situations in which the transmission does not involve "currency"[54] or funds, but instead involves something that the parties to a transaction recognize has value that is equivalent to or can substitute for currency.[55]

FinCEN applied this standard to several common business models involving CVC—including P2P exchangers,[56] hosted wallet providers,[57] "mixers" and "tumblers,"[58] and CVC kiosks (sometimes called "bitcoin ATMs"),[59]—and concluded that all are "money transmitters" subject to compliance obligations under the BSA unless they meet one of the narrow exemptions defined in the BSA Regulations.

4. Decentralization and the Regulatory Framework

In an April 2023 report assessing illicit finance risk in decentralized finance ("DeFi"), the Treasury Department expressly stated that "a DeFi service that functions as a financial institution as defined by the BSA, regardless of whether the service is centralized or decentralized, will be required to comply with BSA obligations, including AML/CFT obligations."[60] The report points out that there is no generally accepted definition for "DeFi," and that many DeFi services have a controlling organization that offer centralized administration and governance support.[61] While acknowledging that determining whether a service is decentralized is a matter of facts and circumstances, the report indicates that "the degree to which a service is decentralized has no bearing on [its BSA] obligations so long as the service meets [the definition of "financial

---

[52] *See Id*. at 2.
[53] *See Id*. at 1.
[54] *See* 31 C.F.R. § 1010.100(m) (defining currency as "[t]he coin and paper money of the United States or of any other country that is designated as legal tender and that circulates and is customarily used and accepted as a medium of exchange in the country of issuance. Currency includes U.S. silver certificates, U.S. notes and Federal Reserve notes. Currency also includes official foreign bank notes that are customarily used and accepted as a medium of exchange in a foreign country.")
[55] FinCEN, FIN-2019-G001, "Application of FinCEN's Regulations to Certain Business Models Involving Convertible Virtual Currencies" (May 9, 2019), at 4, https://www.fincen.gov/sites/default/files/2019-05/FinCEN%20Guidance%20CVC%20FINAL%20508.pdf
[56] *See* 2019 FinCEN CVC Guidance at 14.
[57] *See Id*. at 16.
[58] *See Id*. at 19.
[59] *See Id*. at 17.
[60] *See* Treasury Department, "Illicit Finance Risk Assessment of Decentralized Finance" (April 2023), at 2.
[61] *Id. at* 1.

institution"]."[62] While the degree to which a platform is centralized could impact the service it provides, persons engaging in the activities of "financial institutions" as defined by the BSA, regardless of whether they are centralized or decentralized, will have these obligations, and will similarly have obligations to comply with economic sanctions programs administered and enforced by OFAC.

D. BSA/AML and OFAC Compliance Program

Any Web3 organization that acts in the capacity of a financial institution regulated under U.S. law must be registered to engage in that activity. Organizations that are futures commission merchants or introducing brokers in commodities must register as such with the CFTC.[63] Organizations that are securities exchanges, brokers, dealers, and/or clearing agency must register as such with the SEC.[64] Organizations that are MSBs, including "money transmitters," must register with FinCEN.[65] If a Web3 organization, regardless of whether it is centralized or decentralized, is subject to registration as one or more of the types of financial institution listed above, then the organization is required to comply with the requirements of the BSA and with OFAC sanctions requirements.[66]

Under the BSA, in addition to reporting and recordkeeping requirements, the organization would be required to develop, implement, and maintain an effective, written AML Program that is reasonably designed to prevent the organization from being used to facilitate money laundering and the financing of terrorist activities.[67] FinCEN would expect the organization to promote a "culture of compliance" and implement a written AML Program that has the following four "pillars": policies, procedures and internal controls reasonably designed to assure ongoing compliance, including effective and appropriate KYC and recordkeeping controls; a designated individual responsible for assuring day to day compliance with the AML Program and BSA requirements; training for appropriate personnel, including training in the detection of suspicious transactions; and a process for independent review of the AML Program to ensure that it is adequate – both in structure and implementation.[68]

In addition to the legal requirement to comply with OFAC sanctions regulations, it is a best practice for the organization to develop, implement, and maintain an effective,

---

[62] *Id. at* 1, 2.
[63] 7 U.S.C. § 6d(a).
[64] 15 U.S.C. § § 78e, 78o(a), and 78q-1(b).
[65] *See* 31 U.S.C. § 5330; 31 C.F.R. § 1022.380. The FinCEN registration requirement and other requirements of the BSA are independent obligations. An MSB's failure to register with FinCEN does not relieve an MSB of its obligations under the BSA; likewise, an MSB's registration with FinCEN does not mean that the MSB has fulfilled all of its requirements under the BSA.
[66] *See* 31 C.F.R. § 1010.100 (t)(5).
[67] 31 C.F.R. § 1022.210(a).
[68] 31 C.F.R. § 1022.210(d).

risk-based OFAC Sanctions Compliance Program with key elements that parallel the required elements of AML Programs.[69]

The sections below provide a high-level overview of regulators' supervisory requirements and expectations for BSA AML Programs and OFAC Sanctions Compliance Programs.[70]

1. Culture of Compliance

Senior management, including owners, boards of directors, and senior executives, should foster a culture of compliance.[71] This culture of compliance dictates the basic norms of behavior, knowledge, and transparency under which the management team, employees, and service providers will be held accountable. Management can promote a culture of compliance by setting the "tone at the top" and ensuring that it both messages and takes actions that discourage misconduct and prohibited activities. It is critical for management to provide adequate support and resources for compliance personnel.

2. Risk Assessment

AML and Sanctions Compliance Programs should apply a risk-based approach. One of the central tenets of this approach is for organizations to conduct an "AML Risk Assessment" and a "Sanctions Compliance Risk Assessment" for the purposes of identifying and mitigating potential money laundering, terrorist finance, sanctions evasion, and illicit financial activity risks. The Risk Assessments should consider risks posed by customers, intermediaries, and counterparties; the products and services the organization offers and the channels through which those products are offered; and the geographic locations of the institution, its customers, intermediaries, and counterparties.[72]

The Risk Assessments should be updated periodically, and more frequently as needed to reflect changes in an institution's risk profile or deficiencies identified through audits or regulatory examinations. Changes such as new products and services, increases in transaction volume, and expansion to new jurisdictions are all examples of changes that could introduce new risks.

---

[69] *See* OFAC Compliance Framework at 1.

[70] This overview emphasizes the requirements and expectations that are applicable broadly to all types of "financial institution" (*e.g.*, futures commission merchant, money transmitter, etc.). Additional, more detailed requirements that are specific to the type of "financial institution" and codified under the regulators of the SEC or CFTC may also apply. For clarity and concision, all citations to the BSA Regulations in this section refer to requirements for "money transmitters."

[71] *See* FinCEN, FIN-2014-A007, "Advisory to U.S. Financial Institutions on Promoting a Culture of Compliance" (Aug. 11, 2014), https://www.fincen.gov/sites/default/files/advisory/FIN-2014-A007.pdf; OFAC Compliance Framework at 2.

[72] *See* 31 C.F.R. § 1022.210(b); OFAC Compliance Framework at 3.

The results of the Risk Assessment should be used to develop and apply appropriate internal controls (*i.e.*, policies, procedures, and processes) to mitigate and manage those risks and to better identify and mitigate any gaps in controls.

3. Policies, Procedures, and Internal Controls

Effective AML and Sanctions Compliance Programs should include internal controls, including policies and procedures, in order to identify, interdict, escalate, report (as appropriate), and keep records pertaining to (i) compliance with information collection and recordkeeping requirements and (ii) activity that may be prohibited by the regulations and laws administered by FinCEN and OFAC, respectively.

The purpose of internal controls is to outline clear expectations, define procedures and processes pertaining to compliance (including reporting and escalation chains), and minimize the risks identified by the organization's Risk Assessments. Policies and procedures should be enforced, weaknesses should be identified (including through root cause analysis of any compliance breaches) and remediated, and internal and/or external audits and assessments of the program should be conducted on a periodic basis.

The sections below highlight certain key processes and internal controls that are explicitly or implicitly required or expected to be part of the Program.

a. Customer Identification and Due Diligence

Organizations must maintain, as part of their AML Program, a customer identification or KYC process. When opening an account for, or establishing a service relationship with, a customer, organizations should, at a minimum, verify the customer's identity, to the extent reasonable and practicable, maintain records of the information used to verify such identity, including name, physical address, and other identifying information.

The level of due diligence on customers should follow a risk-based approach, subject to certain regulatory thresholds applicable to different types of financial institutions. Enhanced levels of due diligence may be appropriate for higher-risk customers, high-volume accounts, accounts on which a suspicious activity report has been filed, accounts for non-U.S. persons, accounts for persons in certain geographical jurisdictions identified as high risk, and accounts held on behalf of a third party (e.g., correspondent accounts, "for the benefit of" accounts, etc.).

The organization should also check customers against the Specially Designated Nationals ("SDNs") list and other sanctions lists maintained by OFAC. The organization should use the information collected through diligence and other processes, including normal business processes, to assess whether persons are located in comprehensively sanctioned jurisdictions.[73] Examples include ensuring that shipping

[73] *See* OFAC Virtual Currency Guidance at 13.

or billing address information, IP addresses, or email address suffixes collected during the normal course of a company's business are screened.

b. Suspicious Activity Monitoring and Reporting

Organizations should monitor for transactions that might signify money laundering, terrorist financing, sanctions evasion, or other illegal or criminal activity. An organization must report transactions that it "knows, suspects, or has reason to suspect" are suspicious if the transaction is conducted or attempted by, at, or through the organization and the transaction involves or aggregates to at least $2,000 (for an MSB) or $5,000 (for certain other financial institutions) in U.S. dollars or the equivalent amount in digital assets.[74]

A transaction is "suspicious" if it meets any one of the following five criteria: (i) the transaction involves funds derived from illegal activity; (ii) the transaction is intended or conducted in order to hide or disguise funds or assets derived from illegal activity, or to disguise the ownership, nature, source, location, or control of funds or assets derived from illegal activity; (iii) the transaction is designed, whether through structuring or other means, to evade any requirement in the BSA; (iv) the transaction serves no business or apparent lawful purpose, and the organization knows of no reasonable explanation for the transaction after examining the available facts, including the background and possible purpose of the transaction; or (v) the transaction involves use of the organization to facilitate criminal activity.[75]

Generally, effective suspicious activity monitoring and reporting systems include five key components: (i) identification of potentially suspicious activity (through employee identification, law enforcement inquiries, transaction monitoring systems, or other methods); (ii) investigation and analysis; (iii) determination as to whether a SAR should be filed (including documentation of the decision-making process); (iv) completion and filing of a SAR in a timely manner when appropriate (within 30 days of becoming aware of a suspicious transaction); and (v) reporting any continued suspicious activity by filing additional SARs, as warranted.[76]

An organization's suspicious activity monitoring and reporting processes and systems should be tailored to address the risks it identifies though its risk assessment and the risk profiles of its customers. Examples could include counterparty reporting,

---

[74] 31 C.F.R. § 1022.320(a)(2). The SAR filing threshold is specific to the type of financial institution. For example, the SAR filing threshold for "banks" is $5,000 in funds or other assets. *See* 31 C.F.R. § § 1020.320 (banks).

[75] *See* 31 C.F.R. § 1022.320(a)(2).

[76] *See* FFIEC, "BSA/AML Examination Manual: Assessing Compliance with BSA Regulatory Requirements: Suspicious Activity Reporting" (Feb. 27, 2015), at 61-62, https://bsaaml.ffiec.gov/docs/manual/06_AssessingComplianceWithBSARegulatoryRequirements/04.pdf.

flow of funds reporting, account flagging of suspicious accounts and transactions, and degrees of separation reporting, among others.[77]

Organizations should also implement blockchain analytics tools, tailored to the organization's specific risk profile (as determined through the Risk Assessment), to mitigate digital asset-specific risks.[78] These tools can be used to assess whether a digital asset has substantial exposure to a high-risk or sanctioned jurisdiction, was processed through a mixer or tumbler, was sent to or from darknet markets, was associated with scams/ransomware, was associated with other illicit activity. Additionally, these tools can be used to identify transactions involving wallet addresses or other identifying information (e.g., originator, beneficiary, originating and beneficiary exchanges, and underlying transactional data) associated with sanctioned individuals and entities listed on OFAC sanctions lists or located in sanctioned jurisdictions.

c. Records, Reports, and Law Enforcement Requests

Organizations are required to implement policies, procedures, and internal controls to file required reports,[79] create and retain records,[80] and respond to law enforcement requests.[81] The designated responsible individual (*i.e.*, AML Officer or Sanctions Compliance Officer) has primary day-to-day responsibility for ensuring that these requirements are fulfilled.

d. Funds Transfer and Funds Travel Rule

A specific reporting and recordkeeping topic of interest to organizations that process digital asset transactions is compliance with the Funds Transfer Rule and the Funds Travel Rule. To the extent that any of the organization's transactions constitute a "transmittal of funds"[82] then the organization must comply with the "Funds Transfer

---

[77] *See, e.g.*, FinCEN, *Consent Order In the Matter of Ripple Labs, Inc*., No. 2015-05 (May 5, 2015), "Attachment B: Remedial Framework." (describing transaction monitoring functions to be implemented per settlement agreement with FinCEN).

[78] FinCEN has issued multiple "red flag" advisories listing risks specific to digital assets that, when encountered, may warrant additional scrutiny to help determine whether the activity is suspicious. *See, e.g.*, FinCEN FIN-2019-A003, "Advisory on Illicit Activity Involving Convertible Virtual Currency" (May 9, 2019), https://www.fincen.gov/sites/default/files/advisory/2019-05-10/FinCEN%20Advisory%20CVC%20FINAL%20508.pdf (discussing "red flags" for transactions in convertible virtual currency generally); FIN-2022-Alert001, "FinCEN Advises Increased Vigilance for Potential Russian Sanctions Evasion Attempts" (Mar. 7, 2022), https://www.fincen.gov/sites/default/files/2022-03/FinCEN%20Alert%20Russian%20Sanctions%20Evasion%20FINAL%20508.pdf (highlighting "red flags" for use of convertible virtual currency in potential sanctions evasion activity).

[79] *See* 31 C.F.R. § 1022.210(d)(1)(i)(B).

[80] *See* 31 C.F.R. § 1022.210(d)(1)(i)(C).

[81] *See* 31 C.F.R. § 1022.210(d)(1)(i)(D).

[82] *See* 31 C.F.R. § 1010.100(ddd).

Rule"[83] and the "Funds Travel Rule."[84] Under the recording and recordkeeping aspect of these rules, organizations are required to collect and retain information related to transmittals of funds in amounts of $3,000 or more.[85] Under the transmittal aspect of these rules, organizations must transmit certain information, which the organization is required to collect and retain, to other financial institutions participating in the transmittal.[86]

In the 2019 FinCEN CVC Guidance, FinCEN took the position that transactions in CVC can qualify as "transmittals of funds," and thus fall within the scope of these rules. [87] Compliance with these rules presents unique challenges for the digital asset industry, as blockchains are not designed to send personally identifiable information alongside transactions while simultaneously complying with relevant data privacy obligations. To comply with the rules, virtual asset service providers must implement messaging protocols to send and receive originator and beneficiary information to each other securely.[88]

---

[83] *See* 31 C.F.R. § 1010.410(e).
[84] *See* 31 C.F.R. § 1010.410(f).
[85] *See* 31 C.F.R. § 1010.410(e) (non-bank financial institutions). Among the information that must be collected and retained is (a) name and address of the transmittor; (b) the amount of the transmittal order; (c) the execution date of the transmittal order; (d) any payment instructions received from the transmittor with the transmittal order; and (e) the identity of recipient's financial institution.
[86] *See* 31 C.F.R. § § 1010.410(f).
[87] *See* 2019 FinCEN CVC Guidance at 11. This position could be interpreted as incongruous with the 2013 FinCEN CVC Guidance, where – in the context of analyzing the applicability of the prepaid access rule to CVC – FinCEN opined that if the [prepaid access] rule had intended to cover "funds" denominated in "virtual currency or something else that substitutes for currency, it would have used language. . . like that in the definition of money transmission, which expressly includes. . . 'other value that substitutes for currency.'" 2013 FinCEN CVC Guidance, at FN 18. In this way, the 2013 FinCEN CVC Guidance declined to view CVC as "funds" and instead differentiated between rules that contemplate "funds or the value of funds" (which would not apply to CVC) and those that contemplate "funds or other value that substitutes for currency" (which would apply to CVC). In October 2020, FinCEN and the Federal Reserve proposed to amend the Funds Transfer Rule and Funds Travel Rule to codify the interpretation reflected in the 2019 FinCEN CVC Guidance and also to lower the monetary threshold triggering the rules for certain transactions, but the proposed rule was never finalized by FinCEN (*see* "Threshold for the Requirement To Collect, Retain, and Transmit Information on Funds Transfers and Transmittals of Funds That Begin or End Outside the United States, and Clarification of the Requirement To Collect, Retain, and Transmit Information on Transactions Involving Convertible Virtual Currencies and Digital Assets With Legal Tender Status") (Notice of Proposed Rulemaking), 85 Fed. Reg. 68,005 (Oct. 27, 2020).
[88] An example of an industry-driven solution is the Travel Rule Universal Solution Technology (TRUST), a compliance platform designed by a group of prominent virtual asset service providers formerly known as the U.S Travel Rule Working Group prior to its expansion to non-U.S jurisdictions. Virtual asset service providers who become members of the TRUST platform can securely send the information that is legally required by the Travel Rule to other TRUST platform members.

4. Designation of Individual Responsible For Program

Organizations must designate an individual responsible for coordinating and monitoring day-to-day compliance with the BSA as part of their AML Program obligations, and the appointment of a person similarly responsible for OFAC sanctions compliance is considered a best practice for OFAC Sanctions Compliance Programs.[89] The designated individual should be knowledgeable of the applicable regulatory requirements and have sufficient authority to administer the program. This person is responsible for assuring that the organization properly files required reports (e.g., SARs), creates and retains records in accordance with regulatory requirements, updates the Program as needed to reflect current requirements and supervisory guidance, and provides requisite training (discussed below) to appropriate personnel.[90]

5. Training

An effective training program is an integral component of successful AML and Sanctions Compliance Programs. Training of appropriate personnel in BSA regulatory requirements, in job-specific compliance responsibilities, and in the identification of detection of suspicious transactions is required for all AML Programs, and a parallel sanctions-related training program is a best practice for OFAC Sanctions Compliance Programs.[91] The training program should be provided to all appropriate employees and personnel on a periodic basis (and at a minimum, annually). Organizations should maintain records of training, including copies of training materials, logs with dates of training sessions, and attendance records for employees to which the training was assigned.

6. Audits

Audits assess the sufficiency of an organization's compliance program in light of the organization's activities, the effectiveness of current processes as implemented, and whether there are inconsistencies between these and day-to-day operations. Organizations are required to have a comprehensive and objective testing or audit function within their AML Program, and it is a best practice to have the same for their Sanctions Compliance Program.[92] The audit function should be independent of the activities and business functions that it is charged with reviewing. Organizations are not required to hire an outside consultant to conduct this review, though it may choose to do so, and the in any event, the audit should be performed by persons sufficiently

[89] *See* 31 C.F.R. § 1022.210(d)(2); OFAC Compliance Framework at 2.
[90] *See* 31 C.F.R. § 1022.210(d)(2)(i)-(iii); OFAC Compliance Framework at 2-3.
[91] *See* 31 C.F.R. § 1022.210(d)(3); OFAC Compliance Framework at 7.
[92] *See* 31 C.F.R. § 1022.210(d)(4); OFAC Compliance Framework at 7.

independent from the design and implementation of the compliance programs.[93] The scope and frequency of audits should be commensurate with the organization's risk profile, and in general, an audit should occur at least once annually.

It is the organization's responsibility to enhance its AML and Sanctions Compliance Programs, including all Program-related software, systems, and other technology, to remediate any compliance gaps identified in an audit. Such enhancements might include updating, improving, or recalibrating elements of the Program to account for a changing Risk Assessment or new regulatory requirements or sanctions programs.

E. Enforcement

U.S. federal and state regulators have continued to hold companies engaging in digital asset activities accountable for compliance with applicable law, including the BSA and OFAC sanctions.

1. Penalty Amounts

Civil money penalties for BSA violations are significant. Several factors contribute to the overall size of penalties, including the provision for "per-day" penalty calculations, the government's burden of proof for a "willful" violation,[94] and the automatic inflation adjustment of penalty allocations.

For example, FinCEN may impose a civil money penalty of $67,544 for each willful violation of AML program requirements assessed on or after January 19, 2023. The BSA states that a "separate violation" of the requirement to establish and implement an effective AML program occurs "for each day that the violation continues."[95]

The authorized penalty for each violation of MSB registration requirements assessed on or after January 19, 2023 is $9,966.[96] The BSA states that "each day" a violation of the failure to register as a MSB continues "constitutes a separate violation."[97] FinCEN may impose a penalty not to exceed the greater of the amount involved in the transaction (but capped at $270,180) or $67,544 for each willful violation of SAR requirements

---

[93] *See* FinCEN, FIN-2006-G012, "Frequently Asked Questions – Conducting Independent Reviews of Money Services Business Anti-Money Laundering Programs" (Sept. 22, 2006), https://www.fincen.gov/sites/default/files/shared/Guidance_MSB_Independent_Audits9-21.pdf.

[94] In civil enforcement of the BSA, to establish that a financial institution or individual acted willfully, the government need only show that the financial institution or individual acted with either reckless disregard or willful blindness. The government need not show that the entity or individual had knowledge that the conduct violated the BSA, or that the entity or individual otherwise acted with an improper motive or bad purpose. *See* 31 U.S.C. § 5321(a)(1).

[95] 31 U.S.C. § 5321(a)(1).

[96] 31 U.S.C. § 5330(e)(1); 31 C.F.R. § § 1022.380(e) and 1010.821.

[97] 31 U.S.C. § 5330 and 31 C.F.R. § 1022.380(e).

assessed on or after January 19, 2023.[98] Table 1 at the conclusion of this Chapter shows penalty amounts for violations assessed on or after January 19, 2023.[99]

2. Select Recent Enforcement Actions

a. First Bitcoin "Mixer" Penalized by FinCEN for Violating Anti-Money Laundering Laws

In October 2020, FinCEN assessed a $60 million civil money penalty against Larry Dean Harmon, the founder, administrator, and primary operator of Helix and Coin Ninja, which were mixing and tumbling services, for violations of the BSA and the BSA Regulations.[100]

FinCEN found that Harmon operated Helix as an unregistered MSB from 2014 to 2017. Mr. Harmon subsequently founded, and acted as Chief Executive Officer of, Coin Ninja, which FinCEN found he operated as an unregistered MSB and in the same manner as Helix from 2017 to 2020.

FinCEN's investigation revealed that Mr. Harmon willfully violated the BSA's registration, program, and reporting requirements by failing to register as a MSB, failing to implement and maintain an effective AML Program, and failing to report suspicious activities. Specifically, the investigation demonstrated that Harmon deliberately disregarded his obligations under the BSA and implemented practices to circumvent the BSA's requirements, including by failing to collect and verify customer names, addresses, and other identifiers on over 1.2 million transactions.

The Helix enforcement action also demonstrates the overlap of civil and criminal enforcement for money laundering violations. In addition to the civil enforcement action, Harmon was simultaneously prosecuted in U.S. District Court on charges of conspiracy to launder monetary instruments[101] and operating an unlicensed money transmitting business.[102]

---

[98] 31 U.S.C. § 5321(a)(1); 31 C.F.R. § § 1010.820(i) and 821.
[99] *See* 31 C.F.R. § 1010.821; 88 Fed. Reg. 3311 (Jan 19, 2023) (as corrected by 88 Fed. Reg 7357 (Feb. 3, 2023)).
[100] FinCEN, *Assessment of Civil Money Penalty In the Matter of Larry Dean Harmon d/b/a Helix*, No. 2020-2 (Oct. 19, 2020). The $60 million amount, while sizable, is only a fraction of the maximum penalty amount of $209,144,554 that FinCEN determined was authorized by the BSA and BSA Regulations.
[101] *See* 18 U.S.C. § 1956(h).
[102] *See* 18 U.S.C. § 1960.

b. First Futures Commission Merchant Penalized by FinCEN for Violating Anti-Money Laundering Laws

On August 10, 2021, the CFTC and FinCEN announced $100 million in civil money penalties against BitMEX, a cryptocurrency derivatives exchange, for violations of the Commodity Exchange Act ("CEA")[103] and the BSA.[104]

For over six years, BitMEX publicly represented that its platform was not conducting business with U.S. persons, and therefore was not subject to registration or other requirements under U.S. financial services laws. After investigation, the CFTC and FinCEN found U.S. customers could and did access the BitMEX platform. Among other deficiencies, the CFTC and FinCEN found that BitMEX had failed to implement appropriate policies, procedures, and internal controls to screen for customers that use a virtual private network to access the trading platform and circumvent internet protocol monitoring, which also led to deficiencies in OFAC sanctions screening.

The CFTC alleged, and a U.S. federal district court agreed, that BitMEX operated as an unregistered futures commission merchant ("FCM") and an unapproved Designated Contract Market ("DCM") and Swap Execution Facility ("SEF") in violation of the CEA. Because FCMs are "financial institutions" within the meaning of the BSA, BitMEX was required to implement an AML Program, conduct OFAC sanctions screens, and implement other processes to fulfill the obligations imposed by the BSA Regulations. FinCEN found that BitMEX had willfully violated certain of its obligations under the BSA by failing to implement and maintain a compliant AML Program, failing to implement and maintain a compliant customer identification program, and failing to report certain suspicious activity.

BitMEX was assessed a $100 million civil monetary penalty by the CFTC and FinCEN in connection with the violations. In addition to paying the civil money penalty, BitMEX was required to engage an independent consultant to conduct a historical analysis of its transaction data to determine whether BitMEX needed to file additional SARs on the activity, sometimes referred to as a "SAR lookback." BitMEX was also required to engage an independent consultant to conduct two reviews, including relevant testing, to ensure that it had appropriate policies, procedures, and controls in to ensure that was BitMEX is not operating wholly or in substantial part in the United States.

The CFTC used the BitMEX case as a warning call to the industry: "This case reinforces the expectation that the digital assets industry, as it continues to touch a broader pool of market participants, takes seriously its responsibilities in the regulated financial industry and its duties to develop and adhere to a culture of compliance. . .

---

[103] 7 U.S.C. § § 1 *et seq*.

[104] *See C.F.T.C. v. HDR Global Trading Limited et al*., No. 1:20-cv-08132 (S.D.N.Y), https://www.fincen.gov/sites/default/files/shared/Guidance_MSB_Independent_Audits9-21.pdf; FinCEN, *Assessment of Civil Money Penalty In the Matter of HDR Global Trading Limited, et al*., No. 2021-02 (Aug. 10, 2021).

.The CFTC will take prompt action when activities impacting CFTC jurisdictional markets raise customer and consumer protection concerns."[105] CFTC's position was clear: "Cryptocurrency trading platforms conducting business in the U.S. must obtain the appropriate registration, and must implement robust Know-Your-Customer and Anti-Money Laundering procedures."[106]

c. First NYDFS Enforcement Against New York-Chartered Cryptocurrency Company

In August 2022, the New York Department of Financial Services ("NYDFS") announced that it had entered into a Consent Order with Robinhood Crypto, LLC ("RHC"), in response to what NYDFS described as "compliance deficiencies" in Robinhood's AML Program (as well as programs to comply with cybersecurity regulations and other non-AML regulations).[107]

As a New York-licensed virtual currency entity, RHC was required to establish an effective AML Program that satisfied the standards established by the BSA as well as New York's Transaction Monitoring and Filtering Regulation, known as "Part 504",[108] which establishes marginally higher standards than the BSA and applies only to financial institutions licensed or chartered under New York state law.

After investigation, NYDFS initiated an enforcement proceeding against RHC alleging that RHC's AML Program and Transaction Monitoring Program were insufficient to fully satisfy compliance obligations under applicable requirements. RHC agreed to pay $30 million as a civil monetary penalty and to hire an independent consultant to oversee the remediation of the deficiencies in RHC's AML and Transaction Monitoring Programs.

d. First Parallel Enforcement Actions by FinCEN and OFAC Against Cryptocurrency Company

On October 11, 2022, FinCEN and OFAC announced settlements of $29 million and $24 million, respectively, with Bittrex, Inc. ("Bittrex"), a virtual currency exchange.[109]

---

[105] CFTC Press Release No. 8412-21, "Federal Court Orders BitMEX to Pay $100 Million for Illegally Operating a Cryptocurrency Trading Platform and Anti-Money Laundering Violations" (Aug. 10, 2021), https://www.cftc.gov/PressRoom/PressReleases/8412-21 (quoting CFTC Acting Chairman Rostin Behnam).

[106] *Id.* (quoting Acting Director of Enforcement Vincent McGonagle).

[107] NYDFS, *Consent Order In the Matter of Robinhood Crypto, LLC* (Aug. 1, 2022), https://www.dfs.ny.gov/system/files/documents/2022/08/ea20220801_robinhood.pdf, ("NYDFS RHC Consent Order").

[108] 3 NYCRR Part 504.

[109] *See* FinCEN, *Consent Order In the Matter of Bittrex, Inc.*, No. 2022-03 (Oct. 11, 2022), https://www.fincen.gov/sites/default/files/enforcement_action/2023-04-04/Bittrex_Consent_Order_10.11.2022.pdf; OFAC Enforcement Release, "OFAC Settles with Bittrex, Inc.

The settlements represented the first parallel enforcement actions by FinCEN and OFAC in the virtual currency space.

OFAC alleged that, because of deficiencies related to Bittrex's sanctions compliance procedures, Bittrex had failed to prevent persons apparently located in the Crimea region of Ukraine, Cuba, Iran, Sudan, and Syria from using its platform to engage in virtual currency-related transactions. OFAC further alleged that, based on IP address information and physical address information collected about each customer at onboarding, Bittrex had reason to know that these users were in jurisdictions subject to sanctions, but that at the time of the transactions Bittrex's screening processes failed to identify customers from those sanctioned jurisdictions and stop them from using Bittrex services.

FinCEN alleged that Bittrex had failed to maintain an effective AML Program. Among the areas cited by FinCEN as deficient were Bittrex's allegedly "inadequate and ineffective transaction monitoring," alleged failure to file certain SARs, and alleged failure to file SARs on the transactions involving sanctioned jurisdictions that had been identified by OFAC in its enforcement action. "Virtual asset service providers are on notice that they must implement robust risk-based compliance programs that meet their BSA reporting requirements. . . . FinCEN will not hesitate to act when it identifies willful violations of the BSA."[110]

e. NYDFS and Coinbase Reach Settlement for AML Deficiencies

In January 2023, NYDFS and Coinbase, Inc., a New York state-licensed subsidiary of Coinbase Global, Inc., entered into a consent order to resolve matters related to alleged deficiencies in Coinbase, Inc.'s programs for complying with applicable anti-money laundering and sanctions compliance laws and regulations.[111]

Since 2017, Coinbase, Inc. has been licensed by NYDFS to (i) engage in virtual currency business activities pursuant to New York's "BitLicense" regulatory framework, and (ii) engage in money transmission activities in New York pursuant to the New York Banking Law.

Although some states merely require state-licensed financial institutions to comply with applicable federal laws and regulations, New York-licensed financial institutions such as Coinbase Inc. must also comply with New York regulations that exist in addition to, and do not replace, federal obligations under the BSA and OFAC

---

for $24,280,829.20 Related to Apparent Violations of Multiple Sanctions Programs" (Oct. 11, 2022), https://ofac.treasury.gov/media/928746/download?inline.

[110] Treasury Dep't, "Treasury Announces Two Enforcement Actions for Over $24M and $29M Against Virtual Currency Exchange Bittrex, Inc." (Oct. 11, 2022), https://home.treasury.gov/news/press-releases/jy1006#:~:text=Overview%20of%20FinCEN%20Settlement%20with,its%20potential%20liability%20with%20OFAC(quoting%20FinCEN%20Acting%20Director%20Himamauli%20Das)..

[111] NYDFS, *Consent Order In the Matter of Coinbase, Inc.* (Jan. 4, 2023), https://www.dfs.ny.gov/system/files/documents/2023/01/ea20230104_coinbase.pdf.

regulations.[112] These include (i) the specific AML-related obligations of virtual currency entities set forth in the "Virtual Currency Regulation" (the "BitLicense Regulation")[113] and (ii) the transaction monitoring obligations set out in Part 504 .[114]

According to the Consent Order between NYDFS and Coinbase, Inc., in the course of a routine supervisory examination that covered these New York regulatory obligations, NYDFS examiners identified deficiencies across Coinbase, Inc.'s compliance, including in its KYC procedures, its transaction monitoring system, and its OFAC screening program. The examiners also found that Coinbase, Inc. failed to conduct adequate annual AML risk assessments.

NYDFS expressly recognized that Coinbase, Inc. invested "very substantial time and resources in an effort to remediate its issues and strengthen its Compliance Program more generally."[115] Nevertheless, the total amount to settle the allegations of noncompliance totaled $100 million — a $50 million penalty, plus an agreement by Coinbase Inc. to invest an additional $50 million in its compliance function over two years to remediate the issues and to enhance its compliance program pursuant to an NYDFS-approved plan.

f. FinCEN Issues First Order Pursuant to Combating Russian Money Laundering Act Against Virtual Currency Exchange Bitzlato

In January 2023, FinCEN issued an order identifying virtual currency exchange Bitzlato Limited as a "primary money laundering concern" in connection with Russian illicit finance and prohibited certain transmittals of funds involving Bitzlato by all U.S. domestic "financial institutions" as defined in the BSA.[116] FinCEN determined that Bitzlato played a "critical role" in laundering cryptocurrency by facilitating illicit transactions for ransomware actors operating in Russia, including Conti, a Ransomware-as-a-Service group that has links to the Russian government.

The order is the first use of Section 9714(a) of the Combating Russian Money Laundering Act,[117] which authorizes the Secretary of the Treasury (who has delegated the authority to FinCEN) to order "special measures" to prohibit or impose conditions on transmittals of funds involving a financial institution or account that is of "primary

---

[112] Because of the activities in which Coinbase, Inc. is engaged, it is an MSB under the BSA Regulations and is registered as such with FinCEN. Accordingly, federal law requires Coinbase Inc. to (among other things) develop an AML Program, file SARs, maintain appropriate records, and comply with OFAC sanctions.

[113] *See* 23 NYCRR Part 200.

[114] *See* 3 NYCRR Part 504.

[115] *See* NYDFS RHC Consent Order at 21.

[116] FinCEN, "Imposition of Special Measure Prohibiting the Transmittal of Funds Involving Bitzlato," 88 Fed. Reg. 3919 (Jan. 23, 2023); Press Release, FinCEN, "FinCEN Identifies Virtual Currency Exchange Bitzlato as a 'Primary Money Laundering Concern' in Connection with Russian Illicit Finance" (Jan. 18, 2023), https://www.fincen.gov/news/news-releases/fincen-identifies-virtual-currency-exchange-bitzlato-primary-money-laundering.

[117] P.L. 116-283, as amended by P.L. 117-81.

money laundering concern in connection with Russian illicit finance." This authority is similar in scope and function to the "special measures" authority of Section 311 of the USA PATRIOT Act, but (i) can only be invoked for primary money laundering concerns in connection with Russian illicit finance, (ii) can be implemented via order (without accompanying rulemaking), and (iii) can prohibit or place conditions on certain transmittals of funds.[118]

Effective February 1, 2023, all "covered financial institutions" (all domestic "financial institutions" as defined in the BSA) are prohibited from engaging in the transmittal of funds from or to Bitzlato, or from or to any account or CVC address administered by or on behalf of Bitzlato.[119] FinCEN reminded covered financial institutions, "including, but not limited to, convertible virtual currency (CVC) exchangers," to implement procedures reasonably designed to ensure compliance with the terms of the order and exercise reasonable due diligence to prevent them (or their subsidiaries) from engaging in transmittals of funds involving Bitzlato. If a covered financial institution fails to comply with the order, the covered institution (including, potentially, its officers, directors, employees, and agents) may be liable for civil or criminal penalties.[120]

g. Record-Breaking Civil Money Penalties in FinCEN and OFAC Actions Against Binance

On November 21, 2023, FinCEN and OFAC announced settlements of $3.4 billion and $968 million, respectively, with Binance — at the time of the settlement, the world's largest cryptocurrency exchange — related to multiple violations of the BSA and apparent violations of multiple sanctions programs.[121] The FinCEN and OFAC settlements were part of a global agreement simultaneous with the resolution of related matters with the Department of Justice ("DOJ") and CFTC. The four actions, in aggregate, require Binance to pay over $4.3 billion in criminal forfeiture, penalties, and fines.

FinCEN alleged that Binance violated several different provisions of the BSA between 2017 and 2022. Binance admitted that it willfully operated as an unregistered MSB and willfully failed to establish, implement, and maintain an effective AML

---

[118] Section 9714 of the Combating Russian Money Laundering Act (as amended) can be found in a note to the statute that implements Section 311 of the USA PATRIOT Act. *See* 31 U.S.C. § 5318A.

[119] *See* FinCEN, "FAQs - Section 9714 Order Prohibits Certain Transmittals of Funds Involving Bitzlato" (Jan. 18, 2023), https://www.fincen.gov/sites/default/files/shared/FAQs_Bitzlato%20FINAL%20508.pdf.

[120] *See* 31 U.S.C. § § 5321 and 5322.

[121] *See* FinCEN, *Consent Order Imposing Civil Money Penalty in the Matter of Binance Holdings, et al*., No. 2023-04 (Nov. 21, 2023), https://www.fincen.gov/sites/default/files/enforcement_action/2023-11-21/FinCEN_Consent_Order_2023-04_FINAL508.pdf; OFAC Enforcement Release, "OFAC Settles with Binance Holdings, Ltd. for $968,618,825 Related to Apparent Violations of Multiple Sanctions Programs" (Nov. 21, 2023), https://ofac.treasury.gov/system/files/2023-11/20231121_binance.pdf.

Program by, among other things, failing to perform KYC on a large number of its users until May 2022. Binance admitted that, despite facilitating a significant number of suspicious transactions, it had never filed a SAR with FinCEN as of the date it entered into the settlement agreement. Binance agreed to pay a civil money penalty of $3.4 billion, the largest penalty in the history of FinCEN. The FinCEN settlement agreement also imposes a five-year monitorship and requires significant compliance undertakings, including to ensure Binance's exit from the United States.

OFAC identified 1,667,153 apparent violations of multiple sanctions programs between August 2017 and October 2022.[122] The apparent violations involve transactions in which Binance matched and executed virtual currency trades on its online exchange platform between U.S. person users and users in sanctioned jurisdictions or blocked persons. OFAC assessed a penalty of $968 million, a record amount for OFAC, and required Binance to abide by a series of robust sanctions compliance obligations, including full cooperation with the monitorship overseen by FinCEN.

CFTC alleged that Binance had been functioning as a FCM, foreign board of trade, DCM, and/or SEF; had failed to register with the CFTC as required; and had breached its duties arising out of its alleged status as an FCM to implement effective KYC procedures.[123] To resolve the CFTC's allegations, Binance agreed to enter into a consent order with the CFTC which required Binance to disgorge $1.35 billion in prior gains and pay an additional $1.35 billion civil monetary penalty to the CFTC (with certain payments made by Binance pursuant to FinCEN's civil monetary penalty credited toward the amount owed to the CFTC). The consent order, which was approved by U.S. federal district court in December 2023, permanently enjoined Binance from willfully evading the CEA, acting as an unregistered FCM, operating an illegal digital asset derivatives exchange, and failing to have adequate KYC compliance controls, among other illegal activities.[124]

Binance also reached agreement with the DOJ regarding criminal charges. Binance pleaded guilty to criminal violations concerning unlicensed money transmitting businesses, the BSA, and U.S. sanctions laws, and Binance principal Changpeng Zhao pleaded guilty to intentionally causing Binance to violate the BSA by failing to implement an effective AML Program.[125]

---

[122] *See* OFAC Enforcement Release "OFAC Settles with Binance Holdings, Ltd. for $968,618,825 Related to Apparent Violations of Multiple Sanctions Program" (Nov. 21, 2023), https://ofac.treasury.gov/system/files/2023-11/20231121_binance.pdf.

[123] *See* CFTC, Press Release No. 8825-23, "Binance and Its CEO, Changpeng Zhao, Agree to Pay $2.85 Billion for Willfully Evading U.S. Law, Illegally Operating a Digital Asset Derivatives Exchange, and Other Violations" (Nov. 21, 2023), https://www.cftc.gov/PressRoom/PressReleases/8825-23.

[124] *See* CFTC, Press Release No. 8837-23, "Federal Court Enters Order Against Binance and Former CEO, Zhao, Concluding CFTC Enforcement Action" (Dec. 18, 2023), https://www.cftc.gov/PressRoom/PressReleases/8837-23.

[125] Dep't of Justice, Press Release, "Binance and CEO Plead Guilty to Federal Charges in $4B Resolution" (Nov. 21, 2023), https://www.justice.gov/opa/pr/binance-and-ceo-plead-guilty-federal-charges-4b-resolution?trk=public_post_comment-text.

These actions underscored U.S. regulators' commitment to promoting compliance within the virtual currency industry, including by actively enforcing AML and sanctions laws.

F. Conclusion

Web3 entities or persons that function as "financial institutions" as defined by the BSA – regardless of the level of centralization involved – are required to comply with the BSA, OFAC and sanctions rules, and related AML/CFT regulations. Web3 entities that function as financial institutions, depending on the activities and services involved, may fall under the AML/CFT regulatory frameworks enforced by the SEC, CFTC, federal and state banking authorities, FinCEN, and/or other federal and state agencies that have authority over money transmitters, if they transact in digital assets that are substitutes for currency. In recent years, FinCEN and other U.S. regulators have taken an aggressive enforcement posture against entities that are not compliant with applicable AML/CFT regulations, and policymakers continue to discuss ways to close remaining gaps in the BSA framework, particularly with respect to DeFi.

Table 2: Civil Money Penalties for BSA Violations Assessed On or After January 19, 2023

U.S. Code Citation	Civil Money Penalty Description	Penalties as Last Amended By Statute	Maximum Penalty Amounts (Per Day, If Applicable)
12 U.S.C. § 1829b(j)	Relating to Recordkeeping Violations For Funds Transfers	$10,000	$24,793
12 U.S.C. § 1955	Willful or Grossly Negligent Recordkeeping Violations	$10,000	$24,793
31 U.S.C. § 5318(k)(3)(C)	Failure to Terminate Correspondent Relationship with Foreign Bank	$10,000	$16,771
31 U.S.C. § 5321(a)(1)	General Civil Penalty Provision for Willful Violations of Bank Secrecy Act Requirements	$25,000-100,000	$67,544-$270,180
31 U.S.C. § 5321(a)(5)(B)(i)	Foreign Financial Agency Transaction—Non-Willful Violation of Transaction	$10,000	$15,611
31 U.S.C. § 5321(a)(5)(C)(i)(I)	Foreign Financial Agency Transaction—Willful Violation of Transaction	$100,000	$156,107
31 U.S.C. § 5321(a)(6)(A)	Negligent Violation by Financial Institution or Non-Financial Trade or Business	$500	$1,350
31 U.S.C. § 5321(a)(6)(B)	Pattern of Negligent Activity by Financial Institution or Non-Financial Trade or Business	$50,000	$105,083
31 U.S.C. § 5321(a)(7)	Violation of Certain Due Diligence Requirements, Prohibition on Correspondent Accounts for Shell Banks, and Special Measures	$1,000,000	$1,677,030
31 U.S.C. § 5330(e)	Civil Penalty for Failure to Register as Money Transmitting Business	$5,000	$9,966