King & Spalding

Cryptocurrency: Recent Legal Developments and Outlook

May 2023 Edition

Summary

Federal and state regulators have taken an increased interest in regulating cryptocurrencies, digital assets, and the larger blockchain ecosystem. This landscape is opaque and rapidly evolving, and many industry participants have been left without clear guidance as they seek to innovate while complying with the law. At King & Spalding, a cross-practice team of attorneys specializes in helping clients navigate these very issues. In this publication, we provide an overview of recent legal developments in the crypto and blockchain space, including legislative proposals, key enforcement actions from state and federal agencies, and our outlook for future development.

By:

J.C. Boggs
Andrew Michaelson
Dan Kahan
Ehren Halse
Shas Das
Danielle Pressler
Luke Roniger
Kyle Maury
Diana Liu
Read Mills
John Morrison
Karina Houghton
Lauren Konczos
Hunter McGhee
Spencer Young
Anna Romanova
Gladys Morales

Table of Contents

Introduction

What is Crypto?

When ***Bitcoin: A Peer-to-Peer Electronic Cash System* was** published in 2008 under the pseudonym Satoshi Nakamoto, a quick Google search for "crypto" would have turned up books, articles, and conferences relating to centuries-old study of cryptography. But now, in 2023, "crypto" has become synonymous with "cryptocurrency" and corollary concepts like "digital assets," "tokens," and "NFTs" that live on something called the "blockchain." That same Google search will now generate *millions* of results for cryptocurrency exchanges, bankruptcy proceedings, market trends, and even a recent film.[1] Although "crypto" increasingly permeates our lives and captures headlines, many are still left scratching their heads and wondering: *What exactly is crypto?* At its most basic level, crypto is a method of transferring and recording ownership of digital assets using the blockchain technology pioneered by the Bitcoin white paper.

Primer on Blockchain Technology

Blockchain is a technology framework for transmitting and recording data in which the veracity of the recorded data is ensured by a community of users instead of a central gatekeeper. The decentralization feature is why blockchains are often classified as distributed ledgers. The database for transmitting and recording that encrypted data *is* the blockchain. When the encrypted data is transmitted, it is recorded in a sequentially numbered transaction "block" that has been verified as a true-and-correct record of the data by the community of database users. Once verified, the transaction block is posted to the database and linked to the preceding transaction block to create a chain of recorded data. In some ways, blockchains function much like an Excel spreadsheet with each transaction block serving as a numbered "row" of data; when a new row is added, it is essentially time-stamped to create a historical ledger of all the transactions recorded to the blockchain. In most blockchain implementations, once a block is validated and added to the ledger, that addition cannot be reversed—often referred to as *immutability*.

For most blockchains, anyone is free to join the community of users who maintain the database because the blockchain is made publicly available. Participating in the community of users simply requires downloading the software that maintains a real-time copy of the database (called a "node"). By disseminating independent copies of the blockchain among the community of users, blockchain frameworks ensure the accuracy of transaction records within the database. If one user tries to alter a transaction block on their copy of the database, it would not match up with the copies held by the other users. The accuracy of the transaction records within the blockchain therefore depends on *consensus* among the community of users; the true-and-correct copy of the database is the greatest number of independently identical copies of the blockchain held within the community of users.

Cryptocurrency: Digital Currency on Blockchains

Cryptocurrencies (sometimes referred to as "coins," "crypto," or "tokens") are digital assets on a blockchain that are designed to be fungible stores of value and serve as a medium of exchange. In most cases, cryptocurrencies are native to their own blockchain where they are created and transferred among users (*i.e.*, Bitcoins are only found on the Bitcoin blockchain, Ether lives on the Ethereum blockchain, etc.). To send and receive cryptocurrency, users must create a "wallet"—which can be accessed via software, hardware devices, or hosted wallet platforms—that is essentially an address to which cryptocurrency can be sent. Once

[1] *See* CRYPTO (Lionsgate 2019) (featuring an anti-money laundering analyst for a Wall Street bank who uncovers a massive Bitcoin money laundering scheme).

the cryptocurrency has been received in a user's wallet, the user can access a "private key" that functions like a password for authorizing the cryptocurrency to be sent elsewhere. Cryptocurrencies come into existence one of two ways: (1) they are created over time through "mining" on the blockchain, and/or (2) they are "pre-mined" by the group or entity responsible for the blockchain project, which generates the digital assets when the network is launched and then issues them to users.[2]

Mining Cryptocurrencies and Consensus Mechanisms

Cryptocurrency "miners" validate transaction blocks to be added to the blockchain network. As a reward for doing this work to validate transactions, the software running the network generates and delivers them a set of new coins. Although some blockchains have their own unique method for miners to validate transaction blocks, the two most common methods are (1) Proof-of-Work ("PoW") and (2) Proof-of-Stake ("PoS").[3] Both methods are designed to use economic incentives to ensure miners properly validate transaction blocks and are therefore called *consensus mechanisms*; miners must take on some economic risk to validate/mine a transaction block, which builds consensus in the community of users that the transactions have been properly verified.

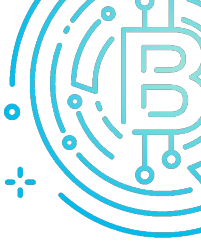
The ***Proof-of-Work*** consensus mechanism is the original means of validating transactions. It was first used by Bitcoin. Under PoW, miners race against each other to solve a difficult cryptographic puzzle that requires a substantial amount of computing power. And with each block mined, the puzzle grows harder to solve and therefore requires even more computing power. PoW therefore pits miners against each other in a competition to build increasingly powerful hardware to be the first to solve the puzzle and validate the transaction block. This requires a substantial investment in high-quality hardware and, of course, a substantial amount of electricity. Competition, market dynamics, and an increase push to renewable and green energy have pushed many crypto mining operations to source electricity from a wide range of cost-effective sources.[4] According to some studies, the power that comes from green sources is between 25% and 60%.[5]

Proof-of-Stake, on the other hand, is a consensus mechanism whereby miners essentially bid on the chance to be the validator for the next transaction block. Typically, PoS requires would-be validators to submit a minimum amount of the native cryptocurrency into a pool, referred to as "staking." The network then selects the next validator based in part on who has staked the largest amount of cryptocurrency and how long it has been in the pool. As a result, network participants are incentivized to hold and stake large amounts of the blockchain's native cryptocurrency in order to maximize their chances of being selected. The winner then validates the next transaction block, although that block is not added to the blockchain until other miners/validators independently confirm its accuracy. If the transaction block is properly validated, then all the participating validators receive a reward in the native cryptocurrency (much like incentives in PoW mining). But if the original validator submits a "bad" or inaccurate transaction block, they will lose some of the cryptocurrency they bid (called "slashing"). Validators are therefore incentivized to validate transaction blocks properly and accurately because they have staked their personal funds for the responsibility of doing so.

Smart Contracts, Tokens, and "dApps"

When the Ethereum blockchain launched in 2015, it marked a significant development in blockchain technology because it introduced the concept of "smart contracts." Smart contracts are essentially software that are stored and run on the blockchain itself, which makes them robust (in that they do not rely on a single point of failure) and difficult to censor or regulate (in that they are not centrally hosted or operated by an identifiable party). When certain conditions are met, the smart contract will execute a set of pre-programmed instructions on the blockchain. Because the execution of smart contracts requires computing power across the network, those

[2] Some blockchains, like Ethereum, have employed a combination of these methods to generate digital assets.
[3] *See* What is "Proof of Work" or "Proof of Stake"?, COINBASE (Nov. 4, 2022), https://www.coinbase.com/learn/crypto-basics/what-is-proof-of-work-or-proof-of-stake.
[4] *See* Sean Stein Smith, Crypto Power Usage Is Helping To Spur Renewable Energy Investments, FORBES (June 5, 2022), https://www.forbes.com/sites/seansteinsmith/2022/06/05/crypto-power-usage-is-helping-to-spur-renewable-energy-investments/?sh=1068b8bc2cb6.
[5] *Id.*



interacting with smart contracts are required to pay fees to node operators (referred to as "gas"), which fluctuate based on network usage and demands on computing resources.

These smart contracts are tethered to the blockchain with "tokens" that can provide the holder of such tokens access to services and/or products built using smart contracts. Smart contracts also form the basis for decentralized applications ("dApps") that run on the Ethereum blockchain and others with similar designs. Example of dApps include token exchanges, blockchain-based games, and decentralized finance platforms.

Decentralized Finance ("DeFi")

Using smart-contract based applications on the Ethereum network, several projects have emerged to offer services and products similar to traditional finance such as lending, derivatives, prediction markets, and market making. Those products and services are typically referred to as "DeFi protocols" because these services are executed through a decentralized smart contract rather than a centralized clearinghouse. Some DeFi protocols, such as the lending protocol Compound, have their own native token, with interest paid to participants using Compound's native token (COMP).[6] In some cases, DeFi protocol tokens also entitle holders to participate in decision-making about the protocol itself (*e.g.,* setting fees for the service). DeFi tokens, including those that are designed to receive rewards and those that are designed to participate in platform governance, can also be traded.[7]

Stablecoins

Stablecoins are a form of cryptocurrency whose value is tied to specific assets (oftentimes fiat currencies like the U.S. dollar). The relationship between the stablecoin's value and the value of the asset to which it is tied is referred to as a "peg." Stablecoins can be collateralized by real-world assets—USDC, for example, is a stablecoin backed by a reserve of U.S. dollars on a 1:1 ratio to maintain its peg of one U.S. dollar per coin. Stablecoins can also be algorithmically tied to fiat currencies and other assets via smart contracts, which can be used to fluctuate the supply of a separate but related token to maintain the stablecoin's peg.[8] For example, DAI is an algorithmic stablecoin that uses a smart contract to ensure its value remains as close to one U.S. dollar as possible by fluctuating the crypto assets serving as collateral based on their price (*i.e.*, it will buy/sell various cryptocurrencies to ensure the value of each DAI token issues is equivalent to $1).[9]

Non-Fungible Tokens (NFTs)

As we explained in our NFT series last year,[10] NFTs are unique digital assets that exist on the blockchain and represent control of a specific asset or convey a set of rights. Unlike cryptocurrencies, NFTs are inherently designed to be non-fungible. They are tied to unique assets on the blockchain and represent a claim of ownership over digital or non-digital assets, such as real estate, artwork, or club membership.[11] NFTs are "minted" on the blockchain using smart contracts, which execute and store data about the NFT on the blockchain. In many ways, the NFT functions as a digital certificate of ownership and provenance on the blockchain.

---

[6] *See, e.g.*, Guide to DeFi Tokens and Altcoins, COINBASE (Nov. 4, 2022), https://www.coinbase.com/learn/crypto-basics/defi-tokens-and-altcoins.

[7] *See, e.g.,* What Are Governance Tokens, BINANCE (Sept. 29, 2022), https://academy.binance.com/en/articles/what-are-governance-tokens; Benedict George, What Is a Governance Token?, COINDESK (Jan. 12, 2022), https://www.coindesk.com/learn/what-is-a-governance-token/.

[8] *See* A Beginner's Guide on Algorithmic Stablecoins, COINTELEGRAPH (Nov. 4, 2022), https://cointelegraph.com/altcoins-for-beginners/a-beginner-s-guide-on-algorithmic-stablecoins.

[9] *See* Milad Mirshahi, What is DAI and how does it work?, FIRI (July 27, 2021), https://firi.com/cryptocurrency/stablecoin-dai/what-is-dai.

[10] *See* Not Your Standard Orange Grove: Non-Fungible Tokens & Securities Laws, KING & SPALDING (Jun. 16, 2021), https://www.kslaw.com/news-and-insights/not-your-standard-orange-grove-non-fungible-tokens-securities-laws; *The Anti-Money Laundering Act and Crypto Collide: Non-Fungible Tokens*, KING & SPALDING (May 18, 2021), https://www.kslaw.com/news-and-insights/the-anti-money-laundering-act-and-crypto-collide-non-fungible-tokens.

[11] *See* How do NFTs work?, ETHEREUM.ORG (Nov. 4, 2022), https://ethereum.org/en/nft/#what-are-nfts.

Year in Review: 2022

Clashing Visions for the Future of Cryptocurrency

In 2022, Congress, regulators, and crypto market participants all wrestled with the same question, albeit from vastly different perspectives: *What do we do with crypto?*

The varying perspectives among these differently situated stakeholders are, unsurprisingly, very different. By May 2022, following the global cryptocurrency market capitalization peak in November 2021 at $2.9 trillion,[12] Congress had introduced more than 50 pieces of crypto-related legislation addressing everything from whether the Federal Reserve should have its own digital currency to which regulatory agency (or agencies) should oversee the crypto market.[13] At the same time, SEC Chairman Gary Gensler continued to assert the importance of SEC oversight over crypto assets and markets, emphasizing how Congress "painted with a broad brush the definition of a security" and asserting that this year's Super Bowl crypto ads reminded him of subprime lenders that placed Super Bowl ads before the 2008 financial crisis.[14]

Meanwhile, Ethereum co-founder Vitalik Buterin and other crypto innovators pondered how blockchain technology could be used to build a "decentralized society" in which individuals have "Soul" accounts on the blockchain and collect "Soulbound Tokens" for real-world achievements (such as graduating from college or having a perfect credit score) to build verifiable identities for people on the internet.[15] Regulators and crypto leaders were thus focused on very different questions, and very different paths, for the technology.

2022 Crypto Winter

By June 2022, the cryptocurrency market cap had fallen by $2 trillion, wiping out nearly 60% of crypto's market value globally and reaching its lowest point since January 2021.[16] Several aspects of this 2022 "crypto winter" have led financial analysts to draw parallels to the 2008 financial crisis.[17] Similar to subprime mortgage lenders in the lead up to 2008, several large crypto institutions held highly leveraged, undercollateralized loans in digital assets intended to be stable compared to the volatility of many cryptocurrencies.[18] Such assets included TerraUSD, an algorithmic stablecoin that was designed to keep its value-per-token pegged at $1.00 by fluctuating the supply of a related token, LUNA, and whose creator advertised 20% interest rates on TerraUSD loaned out through a related DeFi application.[19] Several large crypto funds, including Three Arrow's Capital, held significant positions in TerraUSD using highly leveraged loans from other crypto institutions. When the price of LUNA started falling rapidly over the course of a week, the value of TerraUSD dropped and ended up triggering margin calls from lenders.

[12] Total Cryptocurrency Market Cap, COINMARKETCAP.COM (Nov. 1, 2022), https://coinmarketcap.com/charts/.
[13] *See* Jason Brett, Congress Has Introduced 50 Digital Asset Bills Impacting Regulation, Blockchain, and CBDC Policy, FORBES (May 19, 2022), https://www.forbes.com/sites/jasonbrett/2022/05/19/congress-has-introduced-50-digital-asset-bills-impacting-regulation-blockchain-and-cbdc-policy/?sh=28d4aac34e3f.
[14] SEC. & EXCHG COMM'N, *Prepared Remarks of Gary Gensler On Crypto Markets at the Penn Law Capital Markets Association Annual Conference* (April 4, 2022), https://www.sec.gov/news/speech/gensler-remarks-crypto-markets-040422.
[15] E. Glen Weyl, Puja Ohlhaver, & Vitalik Buterin, Decentralized Society: Finding Web3's Soul (May 11, 2022), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4105763.
[16] Elizabeth Howcroft, Cryptocurrency Market Value Slumps Under $1 Trillion, REUTERS (Jun. 13, 2022), https://www.reuters.com/business/finance/cryptocurrency-market-value-slumps-under-1-trillion-2022-06-13/.
[17] Matt Levine, The Crypto Story, BLOOMBERG BUSINESSWEEK (Oct. 31, 2022), https://www.bloomberg.com/features/2022-the-crypto-story/?leadSource=uverify%20wall#ledgers-bitcoin-blockchains.
[18] *Id.*
[19] Muyao Shen, DeFi App Promising 20% Interest on Stablecoin Deposits Raises Concerns, BLOOMBERG (Mar. 23, 2022), https://www.bloomberg.com/news/articles/2022-03-23/terra-s-promise-of-20-defi-return-raises-sustainability-concern.

When investment fund Three Arrows Capital was unable to meet its margin calls, a credit squeeze ensued that ultimately resulted in bankruptcy for Three Arrows Capital and several of their lenders.[20]

The fall of TerraUSD compounded the effect of decreasing crypto prices brought on by rising interest rates in the U.S., thus causing prices to drop across the entire crypto market.[21]

In early May 2023, the price of Bitcoin hovered around $29,000 compared to its all-time high of nearly $69,000 in November 2021.[22] NFTs have suffered a similar fate during the 2022 crypto winter: resale profit on NFTs fell from $2 billion in the second quarter of 2022 to only $326 million in the third quarter of 2022.[23]

Energy, Mining, and Ethereum 2.0

Rising global energy costs stemming from Russia's war with Ukraine have further hampered crypto miners already battling the current market slump, causing some mining operations to offload cryptocurrency, sell mining equipment, or even shutdown altogether.[24] At the same time, the difficulty in mining Bitcoin has surged to an all-time high, thus requiring even more electricity amid its rising cost.[25]

Meanwhile, U.S. lawmakers led by Sen. Elizabeth Warren have set their sights on energy consumption of crypto mining operations and the corresponding impact on climate change and energy grid stability. In early October 2022, a group of lawmakers opened an investigation into subsidies provided to crypto miners by the Electric Reliability Council of Texas in exchange for a decrease in mining operations during periods of high demand.[26]

Mitigating some of the pressure on crypto mining operations is the Ethereum Merge, which occurred in September 2022. The Merge converted Ethereum's consensus mechanism from Proof-of-Work to Proof-of-Stake by merging the Ethereum Mainnet with a consensus layer called the Beacon Chain to create Ethereum 2.0.

Early estimates suggest Ethereum's transition to PoS may reduce Ethereum's energy consumption by nearly 99.95%.[27]

Positive commentary on the Ethereum merge and the reduction in energy consumption by key U.S. regulators could be a harbinger of future regulatory pressure for PoW-based projects to make a similar switch.[28]

FTX

One of the biggest developments in cryptocurrency in 2022 was spurred by the failure of FTX. FTX, co-founded by Samuel Bankman-Fried in May 2019, operated a cryptocurrency exchange that was, at its peak, the third-largest such platform in operation.[29] FTX also became a critical part of the digital asset ecosystem, acting not only as a counterparty and

---

[20] Matt Levine, The Crypto Story, BLOOMBERG BUSINESSWEEK (Oct. 31, 2022).
[21] *See* Farran Powell and Benjamin Curry, *Crypto Winter Is Here: What You Need To Know*, FORBES (Sept. 2, 2022), https://www.forbes.com/advisor/investing/cryptocurrency/what-is-crypto-winter/.
[22] *See* Bitcoin (BTC), COINBASE (Nov. 4, 2022), https://www.coinbase.com/price/bitcoin#:~:text=Bitcoin%20is%2070.16%25%20below%20the,circulating%20supply%20is%2019%2C197%2C712%20BTC.
[23] NFT Market Report Q3 2022, NONFUNGIBLE (OCT. 17, 2022), https://nonfungible.com/reports/2022/en/q3-quarterly-nft-market-report.
[24] Caitlin Ostroff and Vicky Ge Huang, A Bad Year for Crypto Is a Really Bad One for Crypto Miners, WALL ST. J. (Sept. 12, 2022), https://www.wsj.com/articles/a-bad-year-for-crypto-is-a-really-bad-one-for-crypto-miners-11662970197.
[25] Oliver Knight, Bitcoin Mining Difficulty Surges to All-Time High, Putting Additional Squeeze on Miners, COINDESK (Oct. 10, 2022), https://www.coindesk.com/business/2022/10/10/bitcoin-mining-difficulty-surges-to-all-time-high-putting-additional-squeeze-on-miners/.
[26] Sen. Elizabeth Warren, *Letter to ERCOT re Cryptomining* (Oct. 12, 2022), https://www.warren.senate.gov/imo/media/doc/Letter%20to%20ERCOT%20re%20Cryptomining2.pdf.
[27] Carl Beekhuizen, Ethereum's energy usage will soon decrease by ~99.95%, ETHEREUM FOUNDATION (May 18, 2021), https://blog.ethereum.org/2021/05/18/country-power-no-more.
[28] *See also* The Ethereum Merge: Key Takeaways and Potential Regulatory Impact, KING & SPALDING (Oct. 4, 2022), https://www.kslaw.com/news-and-insights/the-ethereum-merge-key-takeaways-and-potential-regulatory-impact.
[29] *See* The Downfall Of FTX's Sam Bankman-Fried Sends Shockwaves Through The Crypto World, NPR (Nov. 14, 2022), https://www.npr.org/2022/11/14/1136482889/ftx-sam-bankman-fried-shockwaves-crypto.

source of trading liquidity, but also as an investor and acquirer of other firms in the space.[30]

On November 2, 2022, *CoinDesk* reported that the divisions between Alameda Research, the trading firm run by Bankman-Fried, and FTX, the cryptocurrency exchange he operated, were much less clear than many had thought.[31] According to the report, Alameda Research had $14.6 billion in assets, but nearly 40% of those assets consisted of FTX's exchange token, FTT.[32] The reporting caused the markets to focus intensely on FTT, the potentially destabilizing effects on FTX, and the complex relationship between Alameda Research and FTX. Within days of *CoinDesk*'s initial report, on November 8, 2022, Binance, which operates an exchange that competed with FTX, announced that it intended to buy FTX, but walked away from the FTX deal a few days later.[33]

Following the dissolution of those talks, FTX proceeded to seek bankruptcy protection. On November 11, 2022, FTX and approximately 100 affiliates entities (including Alameda Research) commenced voluntary proceedings under Chapter 11 of the U.S. Bankruptcy Code in the District of Delaware.[34] FTX also appointed John J. Ray III, a veteran of several large and complex bankruptcy proceedings, as its Chief Executive Officer.[35]

Law enforcement authorities took action soon after. On December 13, 2022, Bankman-Fried was indicted for "wire fraud, conspiracy to commit wire fraud, conspiracy to commit commodities fraud, conspiracy to commit securities fraud, conspiracy to commit money laundering, and conspiracy to defraud the United States and violate the campaign finance laws."[36] The quick collapse of FTX shook the investor confidence in cryptocurrencies and digital assets, led to several other firms' becoming insolvent,[37] and is expected to bring more attention from regulators to cryptocurrencies.[38]

---

[30] *See* Romain Dillet, Cryptocurrency exchange FTX acquires portfolio tracker Blockfolio, TECHCRUNCH (Aug. 25, 2020), https://techcrunch.com/2020/08/25/cryptocurrency-exchange-ftx-acquires-portfolio-tracker-blockfolio/; *see also* Paul Vigna and Denny Jacob, FTX Strikes Deal With Option to Buy Crypto Lender BlockFi for Up to $240 Million, Wall Street Journal (July 1, 2022), https://www.wsj.com/articles/ftx-strikes-deal-with-option-to-buy-crypto-lender-blockfi-for-up-to-240-million-11656701743.

[31] Ian Allison, Divisions in Sam Bankman-Fried's Crypto Empire Blur on His Trading Titan Alameda's Balance Sheet, COINDESK (Nov. 2, 2022), https://www.coindesk.com/business/2022/11/02/divisions-in-sam-bankman-frieds-crypto-empire-blur-on-his-trading-titan-alamedas-balance-sheet/.

[32] *Id.*

[33] Sage D. Young & Bradley Keoun, The Epic Collapse of Sam Bankman-Fried's FTX Exchange: A Crypto Markets Timeline, COINDESK (Nov. 15, 2022), https://www.coindesk.com/markets/2022/11/12/the-epic-collapse-of-sam-bankman-frieds-ftx-exchange-a-crypto-markets-timeline/.

[34] *See* FTX Trading Ltd., KROLL (May 9, 2023), https://restructuring.ra.kroll.com/FTX/; *see also* Voluntary Petition, Case No. 22-11068-JTD (Del. Bankr, 2022), https://restructuring.ra.kroll.com/FTX/Home-DownloadPDF?id1=MTM1MjM3OQ==&id2=-1.

[35] Elizabeth Napolitano, From Enron to FTX: Wall Street Turnaround Titan John Jay Ray III Takes Reins from FTX CEO Sam Bankman-Fried, COINDESK (Nov. 11, 2022), https://www.coindesk.com/business/2022/11/11/from-enron-to-ftx-wall-street-turnaround-titan-john-jay-ray-iii-takes-reins-from-ftx-ceo-sam-bankman-fried/.

[36] U.S. ATTORNEY'S OFFICE SOUTHERN DISTRICT OF NEW YORK, *United States v. Samuel Bankman-Fried, a/k/a "SBF," 22 Cr. 673 (LAK)* (Jan. 9, 2023), https://www.justice.gov/usao-sdny/united-states-v-samuel-bankman-fried-aka-sbf-22-cr-673-lak.

[37] Lora Kelley, Here's the Latest on the FTX Collapse, THE NEW YORK TIMES (Nov. 28, 2022), https://www.nytimes.com/article/ftx-bankruptcy-crypto-collapse.html.

[38] Ryan Browne, The FTX disaster has set back crypto by 'years' — here are 3 ways it could reshape the industry, CNBC (Dec. 18, 2022), https://www.cnbc.com/2022/12/19/three-ways-the-ftx-disaster-will-reshape-crypto.html.

U.S. Congress

Congress has turned its attention to the subject of digital assets, including cryptocurrency, stablecoins and CBDCs. Congressional interest and oversight is increasing in both Chambers, and a turf war between Congress and key regulatory agencies has emerged.

Congress's attention towards the crypto industry reached a fever pitch following the high-profile collapse of FTX in late 2022. In the wake of the collapse, lawmakers in both chambers reinvigorated focus on potential regulation of cryptocurrency and other digital assets. Senate Banking Chairman Sherrod Brown (D-OH) anticipates a more active role for his Committee, noting that he expects Congress to be "increasingly aggressive" on crypto issues.[39] Following a December Senate Banking Committee hearing, then-Ranking Member Sen. Pat Toomy (R-PA) expressed concern that a lack of clear regulatory oversight in the United States was causing crypto companies to operate in other jurisdictions:

"The absence of legislation that creates the guardrails for regulation and the corresponding absence of any certainty has driven activity offshore to places like the Bahamas. That doesn't always end well for American consumers and others."[40]

Under the new Congress, the timing of Sam Bankman-Fried's arrest was questioned in multiple letters to SEC Chair Gary Gensler by the House Financial Services Committee.[41]

On the House side, House Financial Services Committee Chairman Patrick McHenry (R-NC) expressed the need for new legislation on digital assets and digital asset markets. "For years, I have advocated for Congress to develop a clear regulatory framework for the digital asset ecosystem, including trading platforms," said McHenry in November 2022.

"The recent events show the necessity of Congressional action. It's imperative that Congress establish a framework that ensures Americans have adequate protections while also allowing innovation to thrive here in the U.S."[42]

This echoes Rep. McHenry's January 2022 letter to Financial Services Committee Chairwoman Maxine Waters (D-CA), in which he called for further regulation of cryptocurrency that would give Congress more direct control over emerging policies. Rep. McHenry stated that Congress "should not cede these important issues to regulators such as SEC or CFTC, or to the judicial branch, to determine," and that the "Committee should do its work to appropriately categorize [digital] assets and determine the rules that will govern their use."[43] Reps. Waters and McHenry have a history of collaborating on issues related to digital assets, and many believe that their collaboration will continue into the future. During the December 14, 2022 hearing—the final hearing of the House Financial Services Committee before Rep. McHenry assumed the helm during the 118th Congress—Rep. Waters affirmed their partnership, stating, "I am not only wishing you the best in your chairmanship, but I'm looking forward

[39] Caitlin Reilly, Senate Banking Democrats plan bigger role in crypto legislation, ROLL CALL (Dec. 5, 2022), https://rollcall.com/2022/12/05/senate-banking-democrats-plan-bigger-role-in-crypto-legislation/.
[40] Chris Prentice and Moira Warburton, *U.S. lawmakers scramble to regulate crypto in wake of FTX turmoil*, REUTERS (Dec. 14, 2022), https://www.reuters.com/technology/us-senator-warren-says-crypto-industry-should-follow-money-laundering-rules-2022-12-14/.
[41]0 *See* U.S. HOUSE FINANCIAL SERVICES COMMITTEE, *Letter to SEC on Sam Bankman-Fried Charges* (Feb. 10, 2023) https://financialservices.house.gov/uploadedfiles/2023-02-10_mchenry_huizenga_letter_to_sec_on_sbf_charges_final.pdf ; U.S. HOUSE FINANCIAL SERVICES COMMITTEE, *Letter to SEC on Sam Bankman-Fried Charges* (Apr. 12, 2023) https://financialservices.house.gov/uploadedfiles/pmc_bh_to_sec_re_failure_to_produce_sbf_charges_final.pdf.
[42] U.S. HOUSE FINANCIAL SERVICES COMMITTEE, *McHenry Statement on Recent Events Involving Digital Assets Trading Platforms FTX and Binance* (Nov. 8, 2023), https://republicans-financialservices.house.gov/news/documentsingle.aspx?DocumentID=408466.
[43] *Id.*

to continuing to work—not only on some of the issues that I have alluded to—but certainly on cryptocurrency."[44]

On March 7, 2023, Rep. McHenry reintroduced the Keep Innovation in America Act alongside Rep. Ritchie Torres (D-NY) and a bipartisan group of lawmakers.[45] The bill is intended to "fix the digital asset reporting provisions in the Infrastructure Investment and Jobs Act" and "provide much needed clarity to technology innovators and entrepreneurs."[46] The bill would narrow the definition of "broker" under Section 80603 of the Infrastructure Investment and Jobs Act in an attempt to exempt miners and validators, hardware and software developers, and protocol developers from certain digital asset reporting requirements.[47] It would also "[c]larify what information should be captured by a 'broker' when transferring a digital asset to an account maintained by a non-broker," and provide additional insight into Congress's intent regarding the regulation of digital assets.[48]

Regulators and industry participants have also joined the call for new legislation. In October, SEC Commissioner Hester M. Peirce called on Congress to provide regulatory clarity. "We haven't really done anything besides bringing enforcement actions," said Ms. Peirce. "I think it is a good time for legislation. It's up to Congress to figure out how they want to allocate the regulatory responsibility."[49] Similarly, Coinbase CEO Brian Armstrong published a blog post on December 19th which proposes a regulatory blueprint for cryptocurrencies and other digital assets.[50] The post envisions a scheme that would regulate issuers of stablecoins, create oversight for crypto exchanges, and clearly define which digital assets qualify as commodities and securities.[51] "[My] hope is that the collapse of FTX will be the catalyst we need to finally get new legislation passed," wrote Mr. Armstrong.[52]

Speaking at Consensus 2023 in April, both Rep. McHenry and Sen. Cynthia Lummis (R-WY) signaled that the House Financial Services Committee and House Agriculture Committee would collaborate to introduce legislation during the summer that would oversee the crypto sector in the U.S.[53] Such legislation would likely incorporate elements from the Responsible Financial Innovation Act, which was introduced by Sens. Lummis and Kirsten Gillibrand (D-NY) in 2022. During the Consensus conference, Sen. Lummis announced that she expected to introduce a new version of the bill in the coming weeks.

Recent Proposals and Hearings

Congress closed 2022 with a slate of hearings related to cryptocurrency. In December of last year, the Senate Agriculture Committee,[54] the House Financial Services Committee, and the Senate Banking Committee, all held hearings to examine the state of the digital asset regulatory landscape. In total, Congress held at last 15 hearings focused on cryptocurrency and blockchain policy during 2022.[55] These followed a landmark hearing to close out 2021,

---

[44] Waters, McHenry, Discuss Cryptocurrency and Stablecoin Plans at Final Hearing of 2022, LXR GROUP (Dec. 14, 2022), https://lxrdc.com/waters-mchenry-discuss-cryptocurrency-and-stablecoin-plans-at-final-hearing-of-2022/.

[45] U.S. HOUSE FINANCIAL SERVICES COMMITTEE, *McHenry, Torres, Colleagues Reintroduce Bipartisan Legislative Fix to Digital Asset Reporting Requirements* (Mar. 7, 2023), https://financialservices.house.gov/news/documentsingle.aspx?DocumentID=408642.

[46] *Id.*

[47] Keep Innovation in America Act, 118th Cong. (introduced 2023), https://financialservices.house.gov/uploadedfiles/mchenr_kia.pdf.

[48] Rep. Tom Emmer, *Emmer, McHenry, Colleagues Reintroduce Bipartisan Legislative Fix to Digital Asset Reporting Requirements* (Mar. 7, 2023), https://emmer.house.gov/2023/3/emmer-mchenry-colleagues-reintroduce-bipartisan-legislative-fix-to-digital-asset-reporting-requirements.

[49] Brian Croce, *SEC commissioner calls on Congress to pass crypto regulatory bill*, PENSIONS & INVESTMENTS (Oct. 12, 2022), https://www.pionline.com/regulation/sec-commissioner-calls-congress-pass-crypto-regulatory-bill.

[50] Brian Armstrong, *Regulating Crypto: How we move forward as an industry from here*, COINBASE (Dec. 19, 2022), https://www.coinbase.com/blog/regulating-crypto-how-we-move-forward-as-an-industry-from-here.

[51] *Id.*

[52] *Id.*

[53] Amitoj Singh, *U.S. House Will Have Crypto Bill in 2 Months: Rep. McHenry*, COINDESK (Apr. 28, 2023), https://www.coindesk.com/policy/2023/04/28/us-house-will-have-crypto-bill-in-2-months-mchenry/.

[54] The Senate Agricultural Committee has jurisdiction over the Commodities Futures Trading Commission (CFTC), which regulates the financial derivatives market and will play a critical role in the regulation of digital assets going forward. *See, e.g.*, Sec. IV CFTC, *infra*.

[55] Jason Brett, *2022 Year In Review: Crypto Policy Experiences Massive Turbulence In Congress Amid TerraUSD And FTX Failures*, FORBES (Dec. 23, 2022), https://www.forbes.com/sites/jasonbrett/2022/12/23/2022-year-in-review-crypto-policy-experiences-massive-turbulence-in-congress-amid-terrausd-and-ftx-failures/.

during which chief executives of six cryptocurrency companies testified before the House Financial Services Committee about the state of the industry, as well as future opportunities for development. FTX CEO and founder Samuel Bankman-Fried was among those to testify.

The momentum generated by Congress at the end of 2022 has continued into 2023. Indeed, on February 14, 2023, the Senate Banking Committee held a hearing called "Crypto Crash: Why Financial System Safeguards are Needed for Digital Assets."[56] During the hearing, members heard testimony regarding stablecoin regulation, banking for the crypto industry, consumer protection, and how the regulation of digital assets should be allocated between the SEC and CFTC.

More recently, during an April 18 SEC Oversight hearing held by the House Financial Services Committee, certain members signaled frustration with the SEC's approach to regulation of the crypto industry. Speaking directly to SEC Chair Gary Gensler, Rep. Patrick McHenry accused the SEC of fueling a lack of clarity in the crypto market with a policy of regulation by enforcement, stating that, "You're punishing digital asset firms for allegedly not adhering to the law when they don't know it will apply to them." Rep. Tom Emmer (R-MN) similarly asked the commissioner whether he was concerned that the SEC's approach was "driving this industry out of the United States." In response, Commissioner Gensler defended the SEC's approach, telling the panel that "[a]ll of these companies should come into compliance with the law, and until they do, we will continue to pursue them as the cop on the beat, and investigate and follow the facts and law." Regardless, the frustration displayed by Rep. McHenry and other members of the committee highlight the extent to which they view Congress's role in providing regulatory clarity as a critical one.

On April 27, 2023, Congress hosted a pair of hearings covering various aspects of digital asset regulation. A hearing hosted by the House Financial Services Committee's Subcommittee on Digital Assets, Financial Technology and Inclusion focused on identifying regulatory gaps in the digital asset market structure.[57] A hearing hosted by the House Agricultural Committee's Subcommittee on Commodity Markets, Digital Assets, and Rural Development discussed the regulation of digital asset spot markets.[58]

While 2022 did not see the passage of any major crypto bills, Congress's renewed interest in the industry could be a catalyst for the passage of legislation in 2023. During the 117th Congress, members introduced more than 50 measures relating to cryptocurrency, blockchain, and central bank digital currency (CBDC).[59] Many of these bills have been or will be reintroduced during the coming term, and some may ultimately be passed into laws that will shape the regulatory landscape for cryptocurrency, blockchain and digital assets for years to come. An overview of the most significant among these follows below in "Key Legislative Proposals."

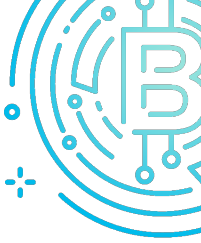
Recent crypto legislative proposals have generally fell into three broad categories. One set of bills have focused on how regulators such as the Securities and Exchange Commission (SEC) and Commodities and Futures Trading Commission (CFTC) will regulate crypto and blockchain tokens. Of those, the "Eliminate Barriers To Innovation Act" (H.R. 1602) passed the House of Representatives in 2021. That bill would have created an SEC and CFTC Working Group on Digital Assets that would report to Congress and help clarify differences in blockchain tokens between the two agencies. In April 2022, a bipartisan group of Representatives introduced a bill aimed at expanding this effort. If passed, the "Digital Commodity Exchange Act", *infra*, would provide

[56] Crypto Crash: Why Financial System Safeguards are Needed for Digital Assets, U.S. HOUSE FINANCIAL SERVICES COMMITTEE (Feb. 14, 2023), https://www.banking.senate.gov/hearings/crypto-crash-why-financial-system-safeguards-are-needed-for-digital-assets.

[57] The Future of Digital Assets: Identifying the Regulatory Gaps in Digital Asset Market Structure, U.S. HOUSE FINANCIAL SERVICES COMMITTEE (Apr. 27, 2023), https://financialservices.house.gov/calendar/eventsingle.aspx?EventID=408718.

[58] The Future of Digital Assets: Identifying the Regulatory Gaps in Spot Market Regulation, U.S. HOUSE COMMITTEE ON AGRICULTURE (Apr. 27, 2023), https://agriculture.house.gov/calendar/eventsingle.aspx?EventID=7604.

[59] Jason Brett, *Congress Has Introduced 50 Digital Asset Bills Impacting Regulation, Blockchain, And CBDC Policy*, FORBES (May 19, 2022) https://www.forbes.com/sites/jasonbrett/2022/05/19/congress-has-introduced-50-digital-asset-bills-impacting-regulation-blockchain-and-cbdc-policy/.



"regulatory oversight for spot digital commodity exchanges, market intermediaries, and stablecoin providers" by building on frameworks that already exist in commodities law.

A second group of proposals has aimed to address distributed ledger technology and the broader use of blockchain technology in other sectors of the economy. Finally, a third tranche of bills has aimed to deal with Central Bank Digital Currencies ("CBDCs"), with policymakers becoming more cognizant of risk to the dollar's primacy due to technological innovations such as stablecoins.

Key Legislative Proposals

Among the flurry of recent legislative proposals aimed at regulating cryptocurrency, digital assets, and use of blockchain technology, a select few stand out. Whichever of these bills are ultimately passed will likely set the tone for regulation of the industry for the foreseeable future. Analysis of each follows below.

Lummis-Gillibrand Responsible Financial Innovation Act

On June 7, 2022, Sens. Kirsten Gillibrand (D-NY) and Cynthia Lummis (R-WY) introduced the Lummis-Gillibrand Responsible Financial Innovation Act ("RFIA"), which aims to create a comprehensive regulatory framework for digital assets with regulatory authority over digital asset spot markets assigned to the CFTC.[60] The bill draws a distinction between digital commodities and securities by looking to the purpose of each asset and the rights or powers it conveys to its holders. Though the RFIA was not passed during 2022, Sen. Lummis recently announced that she and Sen. Gillibrand intend to introduce an updated version of the bill during the summer of 2023.[61] Sen. Gillibrand stated that the new bill would expand on its 2022 predecessor by implementing a broad regulatory framework and taking a "deep dive" on stablecoin regulation.[62]

In its most recent form, the RFIA defines a "digital asset" as a "natively electronic asset that confers economic, proprietary, or access rights or powers; and is recorded using cryptographically secured distributed ledger technology, or any similar analogue."[63] This specifically includes virtual currency and ancillary assets, payment stablecoins, and other securities and commodities.[64]

Most digital assets, including bitcoin and ether, as well as payment stablecoins, would fall into the commodities category and be regulated by the CFTC.[65] In contrast, digital assets that convey a debt or equity interest, liquidation rights, an entitlement to an interest or dividend payment, a profit or revenue share derived solely from the entrepreneurial or managerial efforts of others, or any other financial interest in a business entity would generally be classified as securities and excluded from the CFTC's jurisdiction.[66]

The RFIA attempts to further distinguish between commodities and securities by defining "ancillary assets"[67] and classifying them as commodities. Ancillary assets would be required to furnish disclosures with the SEC twice a year unless they can establish that they have become fully decentralized.

The existing RFIA also contains provisions related to stablecoins. Stablecoin issuers would be required to hold reserves of liquid assets valued at 100% of the face value of all outstanding payment stablecoins, publicly disclose the value and nature of assets backing the stablecoins, and allow asset holders to redeem stablecoins at par in legal tender. New

---

[60] Sen. Kirsten Gillibrand, *Lummis, Gillibrand Introduce Landmark Legislation To Create Regulatory Framework For Digital Assets* (Jun. 7, 2022), https://www.gillibrand.senate.gov/news/press/release/-lummis-gillibrand-introduce-landmark-legislation-to-create-regulatory-framework-for-digital-assets/.

[61] Aislinn Murphy, *Slimmed-down crypto legislation coming in April: senators Lummis, Gillibrand*, FOX BUSINESS (March 2, 2023), https://www.foxbusiness.com/politics/slimmed-down-crypto-legislation-coming-in-april-sens-lummis-gillibrand; Amitoj Singh, *U.S. House Will Have Crypto Bill in 2 Months: Rep. McHenry*, COINDESK (Apr. 28, 2023), https://www.coindesk.com/policy/2023/04/28/us-house-will-have-crypto-bill-in-2-months-mchenry/.

[62] *Id.*

[63] Lummis-Gillibrand Responsible Financial Innovation Act, 118th Cong. (introduced 2023), https://www.gillibrand.senate.gov/wp-content/uploads/imo/media/doc/Lummis-Gillibrand%20Responsible%20Financial%20Innovation%20Act%20%5bFinal%5d.pdf.

[64] *Id.*

[65] *Id.*

[66] *Id.*

[67] Defined as "digital assets which are not fully decentralized, and which benefit from entrepreneurial and managerial efforts that determine the value of the assets, but do not represent securities because they are not debt or equity or do not create rights to profits, liquidation preferences or other financial interests in a business entity."

stablecoin creation provisions would provide a framework for banks and credit unions to create their own stablecoins, and create a special-purpose depository institution charter for issuance of payment stablecoins.

In addition, the RFIA aims to create a workable tax structure for digital assets. A *de minimis* exemption of up to $200 would allow people to transact with virtual currency without having to account for and report income. Furthermore, crypto miners and other validators are excluded from the bill's definition of "brokers," so digital assets obtained from mining and staking would not be considered income until the assets are redeemed for cash.[68] With a new version of the RFIA promised during the summer of 2023, industry participants can expect an expanded regulatory framework, more thorough treatment of stablecoin rules, and a "stronger section" addressing national security and cybercrime.[69]

Financial Technology Protection Act

On April 27, 2023, a bipartisan group of Senators and Representatives introduced the Financial Technology Protection Act.[70] The bill, co-sponsored by Sens. Kirsten Gillibrand and Ted Budd (R-NC) and Congressmen Zachary Nunn (R-IA) and Jim Himes (D-CT), aims to study how criminals might use cryptocurrencies and other digital assets to support illegal activities. If passed, the bill would establish a working group of representatives from the Treasury Department, FinCEN, the IRS, the Office of Foreign Asset Control, the FBI, the DEA, the Department of Homeland Security, the Department of Justice, the Department of State, and the CIA, as well as private sector representatives from financial institutions, analytics firms, and research organizations. This working group would be tasked with providing recommendations to Congress on mitigating the risk of illegal activity in the digital asset space.

Digital Commodities Consumer Protection Act

On August 3, 2022, Sens. Debbie Stabenow (D-MI), John Boozman (R-AR), Cory Booker (D-NJ) and John Thune (R-SD) introduced the Digital Commodities Consumer Protection Act of 2022 ("DCCPA").[71] Like the RFIA, the DCCPA, assigns primary regulatory oversight of the digital asset industry to the CFTC. However, the DCCPA grants the agency broader discretion to (1) determine which digital assets fall under its jurisdiction, and (2) regulate digital asset exchanges.

The DCCPA defines a "digital commodity" as any "fungible digital form of personal property that can be possessed and transferred person-to-person without necessary reliance on an intermediary." These would include "property commonly known as cryptocurrency or virtual currency, such as Bitcoin and Ether." Digital commodities would not include assets such as interests in physical commodities, securities, a "digital form of currency backed by the full faith and credit of the United States," or "any other instrument that the [CFTC] determines not to be a digital commodity." As with the RFIA, digital assets falling into one of the excepted categories would fall outside the CFTC's regulatory jurisdiction.

Under the DCCPA, every digital commodities platform would be required to register with the CFTC as a commodities broker, custodian, dealer, or trading facility. Such platforms would be considered financial institutions under the Bank Secrecy Act. Commodities platforms would also be required to take a number of steps to promote market transparency, such as disclosing information about digital commodities and

---

[68] Sen. Cynthia Lummis, *Lummis, Gillibrand Post Responsible Financial Innovation Act on Github for Comments* (Jun. 22, 2022), https://www.lummis.senate.gov/press-releases/lummis-gillibrand-post-responsible-financial-innovation-act-on-github-for-comments/; Sen. Kirsten Gillibrand, *Lummis, Gillibrand Introduce Landmark Legislation To Create Regulatory Framework For Digital Assets* (Jun. 7, 2022), https://www.gillibrand.senate.gov/news/press/release/-lummis-gillibrand-introduce-landmark-legislation-to-create-regulatory-framework-for-digital-assets.

[69] Aislinn Murphy, *Slimmed-down crypto legislation coming in April: senators Lummis, Gillibrand*, Fox Business (March 2, 2023), https://www.foxbusiness.com/politics/slimmed-down-crypto-legislation-coming-in-april-sens-lummis-gillibrand; Amitoj Singh, *U.S. House Will Have Crypto Bill in 2 Months: Rep. McHenry*, CoinDesk (Apr. 28, 2023), https://www.coindesk.com/policy/2023/04/28/us-house-will-have-crypto-bill-in-2-months-mchenry/.

[70] Nikhilesh De, *Reintroduced Congressional Bill Would Call for Feds to Study Terrorist Uses for Crypto*, CoinDesk (Apr. 27, 2023), https://www.coindesk.com/policy/2023/04/27/reintroduced-congressional-bill-would-call-for-feds-to-study-terrorist-uses-for-crypto/.

[71] Sen. John Boozman, *Boozman, Stabenow, Booker and Thune Introduce Legislation to Regulate Digital Commodities* (Aug. 3, 2022), https://www.boozman.senate.gov/public/index.cfm/2022/8/boozman-stabenow-booker-and-thune-introduce-legislation-to-regulate-digital-commodities.

their risks and providing transaction records to the CFTC upon request.[72] This bill has yet to be reintroduced in 2023.

Digital Commodity Exchange Act

On April 28, 2022, Reps. Ro Khanna (D-CA), Glenn Thompson (R-PA), Tom Emmer (R-MN), and Darren Soto (D-FL) introduced the Digital Commodity Exchange Act ("DCEA"). This bill aims to provide "regulatory oversight for spot digital commodity exchanges, market intermediaries, and stablecoin providers" by "[building] on existing frameworks in existing commodities law."[73]

Under the DCEA, the CFTC would have authority to register and regulate digital asset exchanges for spot and cash digital commodity markets. These "digital commodity exchanges" would be required to register with the CFTC to offer leveraged trading or to list digital commodities that were distributed to individuals before being made available to the public. Non-registered exchanges would be unable to offer these products but could continue to operate under state money transmitter licensing regimes. Registered exchanges would also be required to "monitor trading activity, prohibit abusive trading practices, establish minimum capital requirements, report certain trading information publicly, avoid conflicts of interest, establish governance standards, and adopt cybersecurity measures."

The DCEA also attempts to draw a clean line between the CFTC's and SEC's regulatory authority. The SEC would maintain jurisdiction over securities offerings that involve digital assets as well as digital assets that represent ownership or investment in a business entity. However, digital assets that do not convey rights and obligations typically associated with securities would be considered digital commodities and fall under the CFTC's regulatory regime.

Finally, the DCEA would allow asset-backed stablecoin operators to register with the CFTC as fixed-value digital commodity operators. These operators would be required to disclose essential information about their stablecoins, maintain sufficient reserve backing, mitigate and disclose conflicts of interest, and keep books and records available for examination by the CFTC. Fixed-value digital commodity operators in compliance with these obligations would gain access to a streamlined path to listing their stablecoins on digital commodity exchanges.[74] This bill has yet to be reintroduced in 2023.

Digital Asset Anti-Money Laundering Act

On December 14, 2022, Sens. Elizabeth Warren (D-MA) and Roger Marshall (R-KS) introduced the Digital Asset Anti-Money Laundering Act of 2022 ("DAAMLA"). In contrast to other major crypto bills introduced in 2022, which create regulatory directives that apply primarily to the CFTC, the DAAMLA would impose "know-your-customer" rules to the crypto markets under the watch of the Treasury Department's Financial Crimes Enforcement Network (FinCEN).[75]

Specifically, the Warren-Marshall bill would direct FinCEN to designate digital asset wallet providers, miners, validators, and other facilitators of digital asset transactions as money service businesses (MSBs) under the Bank Secrecy Act (BSA). It would also attempt to extend AML rules and sanctions checks to "unhosted" digital wallets by directing FinCEN to implement a rule that it proposed in December 2020. That rule "would require banks and MSBs to verify customer and counterparty identities, keep records, and file reports in relation to certain digital asset transactions involving unhosted wallets or wallets hosted in non-BSA compliant jurisdictions."

---

[72] Chelsey Cox, *Congress considers crypto consumer protection bill that Sam Bankman-Fried backed before FTX collapse*, CNBC (Dec. 13, 2022), https://www.cnbc.com/2022/12/13/digital-commodities-consumer-protection-act-sam-bankman-fried-ftx-fail.html; U.S. SENATE COMMITTEE ON AGRICULTURE, *Ranking Member Boozman Statement on Digital Commodities Consumer Protection Act of 2022* (Nov. 10, 2022), https://www.agriculture.senate.gov/newsroom/rep/press/release/ranking-member-boozman-statement-on-digital-commodities-consumer-protection-act-of-2022.

[73] Rep. Ro Khanna, *Khanna, Thompson, Emmer, Soto Introduce Bipartisan Digital Commodity Exchange Act of 2022* (Apr. 28, 2022), https://khanna.house.gov/media/press-releases/khanna-thompson-emmer-soto-introduce-bipartisan-digital-commodity-exchange-act.

[74] *Id.*

[75] Sen. Elizabeth Warren, *Warren, Marshall Introduce Bipartisan Legislation to Crack Down on Cryptocurrency Money Laundering, Financing of Terrorists and Rogue Nations* (Dec. 14, 2022), https://www.warren.senate.gov/newsroom/press-releases/warren-marshall-introduce-bipartisan-legislation-to-crack-down-on-cryptocurrency-money-laundering-financing-of-terrorists-and-rogue-nations.

The DAAMLA would also bring a number of additional regulators into the fold to extend and strengthen BSA enforcement and compliance. United States nationals who conduct a transaction in digital assets with a value greater than $10,000 through an offshore account would be required to file a Report of Foreign Bank and Financial Accounts (FBAR) with the Internal Revenue Service. The Treasury Department would be directed to establish "an AML/CFT compliance examination and review process for MSBs." And both the SEC and the CFTC would be directed to establish "AML/CFT compliance examination and review processes" for entities under their respective jurisdictions.[76]

House Draft Stablecoin Bill

On April 17, 2023, one day before an SEC Oversight hearing, the House Financial Services Committee published a draft bill to regulate stablecoins. Like the "Stablecoin TRUST Act," introduced by outgoing Sen. Pat Toomy (R-PA) last year, the House proposal establishes definitions applicable to payment stablecoin issuers. The draft bill would also establish a moratorium on the issuance of stablecoins backed by other cryptocurrencies, during which time the Secretary of the Treasury would conduct and carry out a study on such stablecoins. The House Financial Services Committee's draft stablecoin bill was the first piece of major crypto legislation to be introduced in 2023.

[76] *Id.*; Jamie Crawley, *US Senators Warren, Marshall Introduce Digital Assets Anti-Money Laundering Bill*, COINDESK (Dec. 14, 2022), https://www.coindesk.com/policy/2022/12/14/us-senators-warren-marshall-introduce-digital-assets-anti-money-laundering-bill/.

CFTC

CFTC Jurisdiction, Spot Market Regulatory Gap, and Agenda

In 2016, the CFTC announced that Bitcoin, Ether, and other digital assets are commodities within its jurisdiction.[77] At least one court has recently agreed, holding that "Bitcoin, Ether, [and other digital assets] are encompassed within the broad definition of 'commodity' under the [Commodity Exchange] Act" (CEA).[78] And the CFTC has policed accordingly to date in 2023,[79] with 18 digital asset enforcement actions in 2022, and 20 such actions in 2021.[80]

Notably, however, the CFTC lacks spot market jurisdiction. A statutory fix was recently introduced in the House of Representatives—the Digital Commodity Exchange Act (DCEA) of 2022—to grant the CFTC spot commodity market jurisdiction.[81] Until such legislation is passed, CFTC statutory jurisdiction will be limited to futures contracts: when a commodity is exchanged for cash at a future, non-spot date. That limitation has caught the eye of CFTC Chairman Rostin Behnam, who laments that the CFTC "does not have direct statutory authority to regulate [spot] markets" and instead must *indirectly* regulate spot markets through its anti-fraud/manipulation enforcement authority.[82]

While Chairman Behnam recognizes the CFTC "has historically refrained from exercising its [spot] market authority to its full potential as a policy of restraint,"[83] he nonetheless promised hawkish enforcement to a Senate committee because

"the CFTC is well situated to play an increasingly central role in overseeing the [spot] digital asset commodity market"[84]

by using its enforcement authority through judicial interpretation. In his view, full crypto oversight is the natural evolution of the CFTC's "historical roots in overseeing agricultural markets" to more recently overseeing "precious metals to financial indices and swaps."[85]

Enforcement

CFTC crypto enforcement actions take two forms: regulatory actions and anti-fraud/manipulation actions.

Regulatory violations do not require proof of intent. The CFTC regularly brings regulatory actions to promote registration and compliance from futures commodity merchants (FCM),[86] swap execution facilities (SEF), commodity pool operators (CPO),[87] commodity trading advisors (CTA) and other market participants.[88] Such participants are required to register and to maintain adequate records[89] and reporting systems.[90] Registration failures trigger Bank Secrecy Act (BSA) and know-your-customer (KYC) violations under CFTC Regulation 42.2 and Rule 166.3. Previously, these requirements were rarely enforced, but money-laundering risks in crypto have prompted the CFTC to charge these violations alongside failures to register.

Anti-fraud/manipulation actions are harder to prove given their factual complexity and scienter

[77] *In re BFXNA INC. d/b/a BITFINEX*, CFTC Docket No. 16-19 (June 2, 2016).
[78] Order, *In Re iFinex Inc.*, CFTC Docket No. 22-05 (Oct. 15, 2021) at n.2
[79] *See e.g.*, *CFTC v. Avraham Eisenberg*, CFTC Release No. 8647-23 (Jan. 9, 2023) (alleging price manipulation of a digital asset).
[80] "Annual Report of the Division of Enforcement," CFTC (Nov. 2021), (Nov. 2022).
[81] Digital Commodity Exchange Act of 2022, H.R. 7614, 117th Cong
[82] Rostin Behnam, Chairman, CFTC, *Testimony of Chairman Rostin Behnam Regarding "Examining Digital Assets: Risks, Regulation, and Innovation"* (Feb. 9, 2022)
[83] *Id.*
[84] *Id.*
[85] *Id.*
[86] CEA § 4d(a)(1)
[87] CEA §§ 2(c)(2)(C)(iii)(I)(cc)
[88] CEA § 4m(1)
[89] CEA § 4g
[90] CFTC Regulations 43 and 45

requirements. Still, the CFTC allocates significant resources to punish fraudulent schemes that negatively impact price-discovery and market integrity. In this enforcement role, the CFTC is currently focused on the impact on retail investors.[91] Retail participants are typically unsophisticated and primarily engage in price speculation using "naked" positions. Such vulnerability presents a challenge for regulators because, historically, commodity market participants are sophisticated wholesalers and financial institutions that consume commodities and/or hedge price risks. In response the challenges presented by retail participants in commodities markets, the CFTC brought enforcement actions in spot markets for digital assets despite no direct statutory authority, as highlighted by the Digitex and Steynberg actions, below.

Digital Asset Trading Platforms

In October 2022, the CFTC filed a complaint against digital asset trading platform Digitex LLC, citing (1) regulatory violations for failure to register, and (2) manipulation violations for "pumping" (*i.e.,* manipulating upward) its own token, DGTX.

On the registration side, Digitex allegedly ran an illegal derivatives trading platform because it accepted and used customer funds to execute digital asset futures contracts for its customers without registering under Section 4(a) of the CEA. Digitex's alleged Section 4(a) failure to register as a designated contract market (DCM) participant triggered alleged failures to comply with the BSA and its KYC requirements. These allegations mirror a 2020 CFTC action against crypto exchange BitMEX for registration failures and corresponding BSA/AML program violations.[92] Digitex CEO Adam Todd called KYC measures "stupid" and "ridiculous" because "the real reason for KYC is Big Brother."

As for the manipulation claim, the CFTC alleged Digitex "pumped" (*i.e.*, manipulated upward) its native token, DGTX, to compensate for the "commission-free" trades offered to Digitex customers. Todd issued himself at least 100 million DGTX tokens and allegedly pumped DGTX's price by deploying a "bot" to flood the market with purchase orders on third-party exchanges. Although Todd expected to lose money on the bot's purchase orders (in what the CFTC describes as non-economic trading activity), his scheme was designed such that the native tokens held in DGTX's corporate treasury would (on paper) benefit from the pump and exceed any losses. As further evidence of Todd's intent, the CFTC cited an email in which Todd wrote "DGTX will pop" in connection with a "big public launch" because crypto traders and influencers would "talk about how they trade" on Digitex.

The CFTC has continued enforcement in 2023. On March 27, 2023, the CFTC announced a civil enforcement action charging three entities that operate the Binance platform, and certain principals, with "numerous violations of the Commodity Exchange Act (CEA) and CFTC regulations."[93] The CFTC's complaint alleges that Binance "instructed its employees and customers to circumvent compliance controls in order to maximize corporate profits," "did not require its customers to provide any identity-verifying information before trading on the platform," and "failed to implement basic compliance procedures designed to prevent and detect terrorist financing and money laundering."[94] And on April 11, 2023, the CFTC filed a civil enforcement action alleging a New York resident "fraudulently solicit[ed] retail investors to invest in a digital asset trading fund and with misappropriating at least $1 million in investor assets."[95]

Pooled Digital Asset Investments

In 2022, Cornelius Steynberg and his trading entity, MTI, were charged with operating an unregistered Bitcoin commodity pool for accepting at least $1.7 billion in Bitcoin from upwards of 23,000 individuals in the United States.[96] A commodity pool operator (CPO) is defined as "any person engaged in a business that is of the nature of a commodity pool…who in connection therewith solicits, accepts,

[91] Rostin Behnam, Chairman, CFTC, *Testimony of Chairman Rostin Behnam Regarding "Examining Digital Assets: Risks, Regulation, and Innovation"* (Feb. 9, 2022)
[92] *CFTC v. BitMEX*, CFTC Release No. 8270-20 (Oct. 1, 2020).
[93] *CFTC v. Zhao*, CFTC Release No. 8680-23 (March 27, 2023).
[94] *Id.*
[95] *CFTC v. Russell*, CFTC Release No. 8686-23 (April 11, 2023).
[96] *CFTC v. Steynberg*, CFTC Release No. 8549-22 (June 30, 2022); *see also* Commodity Futures Trading Commission v. Mirror Trading International Proprietary Limited, and Cornelius Johannes Steynberg, Case No. 1:22-cv-635 (W.D. Tex. 2022) (herein "MTI Complaint").

or receives funds… for the purpose of trading in commodity interests."[97] Exceptions to registration apply when (1) CPO participants are registered commodities professionals or otherwise accredited investors (*i.e.*, non-retail investors) or (2) the investment commodities within the CPO are a *de minimis* portion of the total assets.[98]

The CFTC alleged that Steynberg was not exempt from registration because (1) none of the solicited individuals were sophisticated investors and (2) the asset pool consisted primarily of commodities (Bitcoin).[99] However, Steynberg was not charged for his failure to register as a commodity trading advisor (CTA) in connection with his commodity pool because, by statute, CTA regulatory requirements apply only to futures or swaps, not the Bitcoin spot market.

Notably, if the proposed DCEA legislation amends CFTC regulatory jurisdiction to include spot market jurisdiction, current CTA regulations[100] would extend to those who provide spot market commodity advice to 15 or more persons over a rolling 12-month period.

Insider Trading

The CEA prohibits trading commodities "on the basis of material nonpublic information in breach of a pre-existing duty" under CEA Section 6(c)(1) and CFTC Regulation 180.1. Both were modeled after the caselaw articulating SEC's insider trading authority under Section 10(b) and Rule 10b-5 of the Securities Exchange Act. In certain circumstances, the CFTC is cautious to bring insider trading charges where the conduct suggests that informational advantages were proper and promote "price discovery." Further, sophisticated commodities traders rarely owe legal duties to fellow market participants, and absent a duty there can be no improper insider trading. Increased trading of digital assets, however, could spark insider trading cases where duties are owed are violated.

Notably, in July 2022 the SEC and DOJ brought parallel insider trading charges against employees of the crypto exchange Coinbase (discussed in the two following sections), but the CFTC did not. CFTC Commissioner Caroline Pham derided the SEC's Coinbase action as a "striking example of [insider trading] regulation by enforcement."[101]

[97] CEA § 1a(11)
[98] *Id.*
[99] MTI Complaint at 16.
[100] CFTC Regulation 4.14
[101] CFTC, Public Statements & Remarks, *Statement of Commissioner Caroline D. Pham on SEC v. Wahi,* (July, 21, 2022).

Department Of Justice

Throughout 2022 and thus far in 2023, the Department of Justice ("DOJ") has showed an increased interest in the digital asset industry. As explained more fully below, DOJ has articulated its vision of the broader regulatory and enforcement landscape, created task forces aimed a policing the industry, and pursued numerous cryptocurrency and digital asset enforcement actions.

The DOJ Cryptocurrency Framework

In October 2020, the DOJ's Cyber-Digital Task Force published "Cryptocurrency: An Enforcement Framework" (the "Framework"), which set forth the DOJ's perspective at the time on emerging law enforcement issues and challenges in areas involving cryptocurrency.[102] The Framework, which was the second detailed report issued by the Attorney General's Cyber-Digital Task Force (first established in February 2018[103]), was published to "enhance understanding of the associated public safety and national security challenges that these technologies present" in order to mitigate the risks of cryptocurrency.

The Framework explained that many criminal activities involving the use of cryptocurrencies are not new or novel, but that criminals are increasingly leveraging the features of cryptocurrencies to advance and conceal unlawful schemes. These schemes fall into three broad categories:

1) Engaging in ***financial transactions associated with the commission of crimes*** (*e.g.*, financing of terrorism; ransom, blackmail, extortion; raising funds for criminal activity).
2) Engaging in ***money laundering or shielding legitimate activity from tax, reporting, or other legal requirements*** (*e.g.*, money laundering, operating exchanges that do not comply with AML and CFT standards, evading taxes, avoiding sanctions).
3) Committing ***crimes directly implicating the cryptocurrency marketplace*** itself, such as stealing cryptocurrency from exchanges through hacking or using the promise of cryptocurrency to defraud unwitting investors.[104]

The Framework also identifies "key legal authorities and partnerships [DOJ] has relied upon to combat criminal and national security threats involving cryptocurrency."[105] It notes that a "wide variety of federal charges can be brought to bear" on crypto-related criminal conduct, including: mail fraud, 18 U.S.C. § 1341; securities fraud, 15 U.S.C. §§ 78j and 78ff; access device fraud, 18 U.S.C. § 1029; identity theft and fraud, 18 U.S.C. § 1028; illegal sale and possession of firearms, 18 U.S.C. § 921 et seq; possession and distribution of counterfeit items, 18 U.S.C. § 2320; child exploitation activities, 18 U.S.C. § 2251 et seq; possession and distribution of controlled substances, 21 U.S.C. § 841 et seq.; and fraud and intrusions in connection with computers, 18 U.S.C. § 1030. The Framework also noted that DOJ can bring a variety of money laundering charges, including under 18 U.S.C. §§ 1956-57, 1960 and 31 U.S.C. § 5331.

Finally, the Framework also describes certain challenges and strategies for addressing those challenges in connection with emerging threats from crypto-related or crypto-adjacent criminal activity

[102] Attorney General William P. Barr Announces Publication of Cryptocurrency Enforcement Framework, U.S. Dep't of Justice (Oct. 8, 2020), https://www.justice.gov/opa/pr/attorney-general-william-p-barr-announces-publication-cryptocurrency-enforcement-framework.
[103] Attorney General Sessions Announces Publication of Cyber-Digital Task Force Report, U.S. Dep't of Justice (July 19, 2018), https://www.justice.gov/opa/pr/attorney-general-sessions-announces-publication-cyber-digital-task-force-report.
[104] Report of the Attorney General's Cyber Digital Task Force, Cryptocurrency: Enforcement Framework at 18-19, U.S. Dep't of Justice (October 2020), https://www.justice.gov/archives/ag/page/file/1326061/download.
[105] *Id* at 2.

(*e.g.*, crypto exchanges, peer-to-peer exchanges and platforms, crypto kiosks, virtual currency casinos, anonymity enhanced cryptocurrencies, mixers, tumblers, and chain hopping).

DOJ's Enforcement Teams

Building on the publication of the Framework,

> *in October 2021, Deputy Attorney General Lisa O. Monaco announced the creation of the National Cryptocurrency Enforcement Team ("NCET") to "tackle complex investigations and prosecutions of criminal misuses of cryptocurrency, particularly crimes committed by virtual currency exchanges, mixing and tumbling services, and money laundering infrastructure actors."*[106]

According to the DOJ,

> *the NCET was established to "deter, disrupt, investigate, and prosecute criminal misuse of cryptocurrency, as well as to recover the illicit proceeds of those crimes whenever possible,"*

while also "foster[ing] the development of expertise in cryptocurrency and blockchain technologies across all aspects of the Department's work."

In February 2022, the DOJ announced that Eun Young Choi would serve as first Director of NCET, leading the department's cryptocurrency enforcement team.[107] As an Assistant United States Attorney in the Southern District of New York, Choi served as lead prosecutor in a variety of cases, including the case against a Russian hacker who helped steal information from more than 80 million JPMorgan & Chase Co customers.[108]

The same day, the DOJ also announced the FBI's new Virtual Asset Exploitation Unit ("VAEU"), a specialized team of cryptocurrency experts dedicated to providing analysis, support, and training across the FBI, as well as innovating its cryptocurrency tools to stay ahead of future threats.[109]

Attorney General Report Regarding Executive Order 14067

On March 9, 2022, President Joe Biden issued Executive Order 14067 (the "Executive Order") to develop frameworks and policy recommendations that advance six key priorities: consumer and investor protection; financial stability; illicit finance; U.S. leadership in the global financial system and economic competitiveness; financial inclusion; and responsible innovation.[110]

Shortly after this announcement, in September 2022, U.S. Attorney General Merrick Garland issued a report pursuant to Section 5(b)(iii) of Executive Order 14067 ("September Report"), which addressed the role of law enforcement in detecting, investigating, and prosecuting criminal activity related to digital assets. The report also established the nationwide Digital Asset Coordinator ("DAC") Network to further the Department's efforts in combatting criminal activity relating to digital assets.[111] According to the DOJ, the DAC Network, which comprises over 150 designated federal prosecutors from U.S. Attorneys' Offices and across the department's litigating components, will serve as the primary forum for prosecutors to obtain and disseminate specialized training, technical expertise, and guidance about the investigation and prosecution of digital asset crimes. Eun Young Choi chaired the DAC Network's first meeting on September 8, 2022.[112] The DAC Network

---

[106] Deputy Attorney General Lisa O. Monaco Announces National Cryptocurrency Enforcement Team, U.S. Dep't of Justice (Oct. 6, 2021), https://www.justice.gov/opa/pr/deputy-attorney-general-lisa-o-monaco-announces-national-cryptocurrency-enforcement-team.

[107] Justice Department Announces First Director of National Cryptocurrency Enforcement Team, U.S. Dep't of Justice (Feb. 17, 2022), https://www.justice.gov/opa/pr/justice-department-announces-first-director-national-cryptocurrency-enforcement-team.

[108] DOJ Names Eun Young Choi to Lead Crackdown on Cryptocurrency Crimes, Newsweek (Feb. 17, 2022), https://www.newsweek.com/feds-announce-new-teams-enforce-investigate-cryptocurrency-crimes-1680349.

[109] U.S. Dep't of Justice, *supra* at 107.

[110] Justice Department Announces Report on Digital Assets and Launches Nationwide Network, U.S. Dep't of Justice (Sept. 16, 2022), https://www.justice.gov/opa/pr/justice-department-announces-report-digital-assets-and-launches-nationwide-network.

[111] *Id.*

[112] *Id.*

will work alongside the NCET, which is involved in investigations of Hydra, Bitfinex, Helix and BitMEX.[113]

Attorney General Garland explained these specialized teams within DOJ "must work in tandem with departments and agencies across government to prevent and disrupt the exploitation of these technologies to facilitate crime and undermine our national security," and that these efforts "reflect the commitment of the Justice Department and our law enforcement and regulatory partners to advancing the responsible development of digital assets, protecting the public from criminal actors in this ecosystem, and meeting the unique challenges these technologies pose."[114]

The White House separately indicated these "efforts are part of a larger, collaborative effort across government agencies" to develop frameworks and policy recommendations that advance six key priorities identified in the EO.[115]

The September Report identifies three priority proposals:

1) Extending the existing prohibition against tipping off suspects to ongoing investigations to virtual asset service providers ("VASPs") that operate as money services businesses.[116]

2) Strengthening federal law prohibiting operation of unlicensed money transmitting businesses by increasing penalties, confirming applicability to digital asset technologies, and codifying existing case law holding only general intent is required.[117]

3) Extending the statute of limitations for digital asset crimes from 5 to 10 years, and providing longer tolling period where the U.S. government has requested foreign evidence, to account for the complexities of digital assets-related investigations.[118]

Effectuating these proposals would increase both the DOJ's power to investigate and prosecute cryptocurrency and digital asset crimes as well as the risks to financial institutions involved in the transmission of digital assets and cryptocurrencies.

The same day the September Report was published, the White House published a fact sheet summarizing the nine reports issued pursuant to the Executive Order. The White House explained that—while monetary losses from digital asset scams were nearly 600 percent higher in 2021 than in 2020—the nine reports "articulate a clear framework for responsible digital asset development and pave the way for further action at home and abroad."[119]

Through the creation of DAC, NCET, and VAEU, the DOJ committed to increasing its resources and capacity to police the digital asset industry. In 2023, the DOJ has dedicated resources focused on expanding its ability to conduct multiyear efforts to address cyber threats and to build cyber investigative capabilities at FBI field divisions nationwide. Specifically, these investments include "an additional $52 million for more agents, enhanced response capabilities, and strengthened intelligence collection and analysis capabilities," and "are in line with the Biden Administration's strategy that emphasizes disruptive activity and combatting the misuse of cryptocurrency."[120]

Enforcement Actions

Fraudulent Digital Asset Schemes

Since the creation of DAC, NCET, and VAEU, the DOJ has pursued a variety of enforcement actions across the digital asset industry. In February 2022, the DOJ announced a landmark seizure of 94,000 Bitcoin valued at over $3.6 billion, linked to the 2016

[113] Crystal Kim, Treasury and Justice reports tackle crypto crime, Axios (September 19, 2022), https://www.axios.com/2022/09/19/treasury-justice-reports-crypto-crime-biden-framework.
[114] U.S. Dep't of Justice, *supra* at 110.
[115] *Id.*
[116] The Report of the Attorney General Pursuant to Section 5(b)(iii) of Executive Order 14067: The Role Of Law Enforcement In Detecting, Investigating, And Prosecuting Criminal Activity Related To Digital Assets, U.S Dep't of Justice (Sept. 6, 2022), https://www.justice.gov/ag/page/file/1535236/download.
[117] *Id.*
[118] *Id.*
[119] White House Releases First-Ever Comprehensive Framework for Responsible Development of Digital Assets, The White House, https://www.whitehouse.gov/briefing-room/statements-releases/2022/09/16/fact-sheet-white-house-releases-first-ever-comprehensive-framework-for-responsible-development-of-digital-assets/.
[120] Budget of the U.S. Government, Fiscal Year 2023, The White House, https://www.whitehouse.gov/wp-content/uploads/2022/03/budget_fy2023.pdf.

hack of the crypto exchange Bitfinex as well as the arrest of a husband-and-wife team on money laundering charges. The couple allegedly conspired to launder bitcoin stolen after a hacker broke into Bitfinex and initiated more than 2,000 unauthorized transactions. At the time, this was the largest seizure of cryptocurrency and the largest single financial seizure in the DOJ's history.[121]

The DOJ's second-largest seizure of cryptocurrency ($3.36 billion of Bitcoin) came in November 2022. The DOJ seized the Bitcoin from a man who "unlawfully obtained" more than 50,000 bitcoin from the illegal Silk Road marketplace that the FBI shut down in 2013. James Zhong of Gainesville, Georgia, pleaded guilty for the Bitcoin theft.[122]

As with its enforcement work outside the digital asset context, DOJ works closely with other agencies in pursuing cryptocurrency-related matters. One example of the DOJ's cross-agency collaborations is the 2022 Bitcoin Mercantile Exchange ("BitMEX") prosecutions. The indictment accused the four BitMEX defendants—three out of four of whom are outside the United States—of BSA violations for willfully failing to establish, implement, and maintain AML and KYC controls. In February 2022, the BitMEX founders ultimately pleaded guilty to violating the BSA.[123]

Cases like these demonstrate that the DOJ "can follow money across the blockchain, just as we have always followed it within the traditional financial system," said Kenneth Polite, assistant attorney general of the DOJ's Criminal Division, and that cryptocurrency is "not a safe haven for criminals," according to Deputy Attorney General Monaco.[124]

Indeed, in June 2022, the DOJ announced four enforcement actions in California and Florida involving allegations of cryptocurrency related fraud. These enforcement actions show the breadth of potential conduct that may expose industry players to regulatory and enforcement risk. In these enforcement actions, the DOJ alleged: (1) a wide-ranging "rug pull" scheme related to NFTs; (2) a fraudulent investment fund trading on cryptocurrency exchanges; (3) a Ponzi scheme involving the sale of unregistered cryptocurrency instruments; and (4) a fraudulent initial coin offering.[125]

Coinbase: Insider Trading Case

Then, on July 21, 2022, the DOJ announced it had charged three individuals in the first ever cryptocurrency insider trading tipping scheme.[126] The indictment alleged that Ishan Wahi, a former product manager at Coinbase Global, Inc. ("Coinbase"), his brother Nikhil Wahi, and his friend Sameer Ramani, netted about $1.5 million in illegal profits. A few months later, Nikhil Wahi pleaded guilty to one count of conspiracy to commit wire fraud as part of a scheme to commit insider trading in cryptocurrency assets by using confidential Coinbase information about which crypto assets were scheduled to be listed on Coinbase's exchanges.[127] To conceal his purchase, Nikhil Wahi used accounts at centralized exchanges held in the names of others, and transferred funds, crypto assets, and proceeds of their scheme through multiple anonymous Ethereum blockchain wallets. He also regularly created and used new Ethereum blockchain wallets without any prior transaction history in order to further conceal his involvement in the scheme.[128] This case may set a precedent for the government's pursuit of wire fraud in cryptocurrency insider trading cases, which the government has argued does not require proof that digital assets are securities. In February 2023, Ishan

[121] Two Arrested for Alleged Conspiracy to Launder $4.5 Billion in Stolen Cryptocurrency, U.S. Dep't of Justice (Feb. 8, 2022), https://www.justice.gov/opa/pr/two-arrested-alleged-conspiracy-launder-45-billion-stolen-cryptocurrency.
[122] U.S. Attorney Announces Historic $3.36 Billion Cryptocurrency Seizure And Conviction In Connection With Silk Road Dark Web Fraud, U.S. Dep't of Justice (Nov. 7, 2022), https://www.justice.gov/usao-sdny/pr/us-attorney-announces-historic-336-billion-cryptocurrency-seizure-and-conviction.
[123] Founders of Cryptocurrency Exchange Plead Guilty To Bank Secrecy Act Violations, U.S. Dep't of Justice (Feb. 24, 2022), https://www.justice.gov/usao-sdny/pr/founders-cryptocurrency-exchange-plead-guilty-bank-secrecy-act-violations.
[124] U.S. Dep't of Justice, *supra* at 122.
[125] Justice Department Announces Enforcement Action Charging Six Individuals with Cryptocurrency Fraud Offenses in Cases Involving Over $100 Million in Intended Losses, U.S. Dep't of Justice (June 30, 2022), https://www.justice.gov/usao-cdca/pr/justice-department-announces-enforcement-action-charging-six-individuals-cryptocurrency.
[126] Three Charged In First Ever Cryptocurrency Insider Trading Tipping Scheme, U.S. Dep't of Justice (July 21, 2022), https://www.justice.gov/usao-sdny/pr/three-charged-first-ever-cryptocurrency-insider-trading-tipping-scheme.
[127] *Id.*
[128] *Id.*

Wahi pleaded guilty to two counts of conspiracy to commit wire fraud.[129]

Bitconnect: SDNY Touting Allegations

The DOJ has remained active in 2023. In January 2023, the Southern District of California ordered that "over $17 million in restitution be distributed to approximately 800 victims from over 40 different countries due to their investment losses in BitConnect, a massive cryptocurrency investment scheme, which defrauded thousands of investors worldwide."[130] According to the DOJ, BitConnect's U.S.-based promoter "touted BitConnect's purported proprietary technology, known as the 'BitConnect Trading Bot' and 'Volatility Software,' as being able to generate substantial profits and guaranteed returns by using investors' money to trade on the volatility of cryptocurrency exchange markets," but "[i]n truth . . . BitConnect operated a textbook Ponzi scheme by paying earlier BitConnect investors with money from later investors."[131]

Mango Markets: Alleged Commodities Fraud, Market Manipulation

In February 2023, the DOJ filed criminal charges in New York against a man for alleged "commodities fraud, commodities market manipulation, and wire fraud charges in connection with the manipulation of the Mango Markets decentralized cryptocurrency exchange."[132] Mango Markets, which is run by the Mango Decentralized Autonomous Organization that offers its own crypto token MNGO, allows investors to "purchase and borrow cryptocurrencies and cryptocurrency-related financial products."[133] Holders of the MNGO token are "allowed to vote on changes to the Mango Markets platform and issues related to the governance of the Mango DAO."[134] DOJ alleged the man "engaged in a scheme to fraudulently obtain approximately $110 million worth of cryptocurrency from the cryptocurrency exchange Mango Markets and its customers and achieved this objective by artificially manipulating the price of certain perpetual futures contracts."[135]

Forsage: Alleged DeFi Scheme

Also in February 2023, a federal grand jury returned an indictment in the District of Oregon that charged four founders of Forsage, a "purportedly decentralized finance ('DeFi') cryptocurrency investment platform, for their roles in a global Ponzi and pyramid scheme that raised approximately $340 million from victim-investors."[136] Court documents alleged that the defendants "coded and deployed smart contracts that systematized their combined Ponzi-pyramid scheme on the Ethereum (ETH), Binance Smart Chain, and Tron blockchains," but "[a]nalysis of the computer code underlying Forsage's smart contracts allegedly revealed that, consistent with a Ponzi scheme, as soon as an investor invested in Forsage by purchasing a 'slot' in a Forsage smart contract, the smart contract automatically diverted the investor's funds to other Forsage investors, such that earlier investors were paid with funds from later investors."[137]

FTX

As noted above, throughout 2023, the DOJ and SEC have pursued ongoing investigations of FTX, one of the biggest crypto exchanges in the world, and its co-founder Sam Bankman-Fried. FTX filed for bankruptcy on November 11, 2022. Before the collapse, FTX was reportedly worth about $16 billion. FTX lent billions of dollars of customer assets to fund risky bets by its affiliated trading firm, Alameda Research. When Changpeng Zhao, founder and CEO of Binance, announced that Binance would sell its hoard of FTT tokens (a token created as part of FTX's trading network) for "risk management" purposes, investors withdrew money from FTX, setting the stage for the company's implosion.

---

[129] Former Coinbase Insider Pleads Guilty In First-Ever Cryptocurrency Insider Trading Case, Dep't of Justice (Feb. 7, 2023), https://www.justice.gov/usao-sdny/pr/three-charged-first-ever-cryptocurrency-insider-trading-tipping-scheme.
[130] Crypto Fraud Victims Receive Over $17 Million In Restitution From BitConnect Scheme, U.S. Dep't of Justice (Jan. 12, 2023), https://www.justice.gov/opa/pr/crypto-fraud-victims-receive-over-17-million-restitution-bitconnect-scheme.
[131] *Id.*
[132] Man Charged in $110 Million Cryptocurrency Scheme, U.S. Dep't of Justice (Feb. 2, 2023), https://www.justice.gov/opa/pr/man-charged-110-million-cryptocurrency-scheme.
[133] *Id.*
[134] *Id.*
[135] *Id.*
[136] Forsage Founders Indicted in $340M DeFi Crypto Scheme, U.S. Dep't of Justice (Feb. 22, 2023), https://www.justice.gov/opa/pr/forsage-founders-indicted-340m-defi-crypto-scheme.
[137] *Id.*

SEC

As of 2023, the SEC remains focused on all things crypto and is increasingly shifting its focus towards crypto exchanges. In April 2023, SEC Chair Gary Gensler delivered prepared remarks to the House Financial Services Committee in which he expressed his view that

> *Congress "gave the Commission a mandate to protect investors, regardless of the labels or technology used" and that "[n]othing about the crypto markets is incompatible with the securities laws."*[138]

In Chair Gensler's view, "[g]iven that most crypto tokens are securities," it follows that many crypto intermediaries, such as crypto exchanges, are facilitating transactions in securities and therefore must register with the SEC.[139]

In 2022, the SEC essentially doubled the size of its Crypto Assets and Cyber Unit, and there are now fifty positions in the unit *dedicated* to cases involving crypto markets and cyber-related threats. Since the Crypto Assets and Cyber Unit was created in 2017, it has brought more than eighty enforcement actions resulting in more than $2 billion in monetary relief.[140]

Enforcement Actions

As detailed below, the SEC's enforcement actions range from unregistered crypto asset offerings and platforms to various fraud schemes. All told, the SEC's appetite to bring enforcement actions shows no signs of slowing.

Unregistered Securities under Howey

A key issue pervading SEC enforcement actions is whether certain crypto asset offerings constitute "securities" under the Supreme Court's *Howey* Test.[141] In a notable ruling in late 2022, the U.S. District Court for the District of New Hampshire granted the SEC's motion for summary judgment against LBRY, Inc., finding that LBRY offered and sold LBC as a security in violation of the registration provisions of the federal securities laws.[142] Crucially—as many cryptocurrencies are arguing in their ongoing administrative and litigation proceedings—the Court held that LBRY did not have a fair notice defense as to the application of those laws for its offer and sale of "LBRY Credits" or "LBC," its crypto asset "securities."

Similar to other cases involving the unregistered sale of securities, the complaint alleged that, from at least July 2016 to February 2021, LBRY sold crypto asset securities without filing a registration statement for the offering, and further denied prospective investors the information required for such an offering.[143] The sale resulted in approximately $12.2 million in proceeds.

In its ruling, the Court only briefly addressed LBRY's argument that LBC was predominately purchased as a utility token, noting that "[n]othing in the case law suggests that a token with both consumptive and speculative uses cannot be sold as an investment contract."[144] Instead, the Court focused specifically on

---

[138] Gary Gensler, Chair, Sec. & Exch. Comm'n, Testimony of Chair Gary Gensler Before the United States House of Representatives Committee on Financial Services (Apr. 18, 2023), https://www.sec.gov/news/testimony/gensler-testimony-house-financial-services-041823.

[139] *Id.*

[140] Press Release, Sec. & Exch. Comm'n, SEC Nearly Doubles Size of Enforcement's Crypto Assets and Cyber Unit (May 3, 2022), https://www.sec.gov/news/press-release/2022-78. The Division of Corporation Finance also added the Office of Crypto Assets to its Disclosure Review Program this past fall to better focus its review of filings involving crypto assets. *See* Press Release, Sec. & Exch. Comm'n, SEC Division of Corporation Finance to Add Industry Offices Focused on Crypto Assets and Industrial Applications and Services (Sept. 9, 2022), https://www.sec.gov/news/press-release/2022-158.

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

[142] Memorandum and Order, *SEC v. LBRY, Inc.*, No. 1:21-cv-00260-PB (D.N.H. Nov. 7, 2022).

[143] Complaint, *SEC v. LBRY, Inc.*, No. 1:21-cv-00260-PB (D.N.H. Mar. 29, 2021).

[144] Memorandum and Order, *SEC v. LBRY, Inc.*, No. 1:21-cv-00260-PB (D.N.H. Nov. 7, 2022).

LBRY's substantial holdings of LBC and representations it made to prospective purchasers, concluding that investors would reasonably expect to profit from investments in LBC based on LBRY's efforts.

The SEC has brought similar charges concerning other digital assets. In 2020, for instance, the SEC initiated a lawsuit against Ripple, alleging that it conducted an unregistered offering of XRP.[145] Ripple has argued that its sales of XRP do not constitute "investment contracts." And in its briefing on summary judgment, Ripple argued that in *Howey* itself and in cases both preceding and following it, courts found "investment contracts" only where there was (a) a contract, (b) imposing post-contractual obligations, and (c) profit-sharing.[146] Ultimately, Ripple has contended that there cannot be an "investment contract" without a contract. Summary judgment is pending before Judge Torres in the Southern District of New York. The Court's decision will impact the future of cryptocurrency regulations and determine whether XRP is a security to be regulated under the SEC, or a commodity.

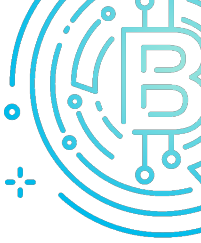
In another example from 2022, the SEC alleged that Dragonchain conducted an unregistered offering of securities. The SEC specifically noted that Dragonchain's "marketing materials explicitly stated that the value of the token would increase as adoption of its technology grew," and that "the value of DRGNs [its cryptocurrency] would rise as the Dragonchain 'ecosystem' matured."[147] Dragonchain's founder also allegedly made statements regarding the token, and the company maintained social media accounts where DRGNs' "investment value, trading prices, and market capitalization" were discussed.

Instead of fighting this issue in court, some cryptocurrency companies have settled with the SEC. For instance, in September 2022, Sparkster entered a cease and desist order with the SEC involving violations of the offering provisions of the federal securities laws.[148] The SEC alleged that Sparkster raised approximately $30,000,000 from almost 4,000 investors through a "presale" and "crowdsale" with the goal of increasing the value of "SPRK" tokens, making them available on a crypto asset trading platform, and continuing to improve the company's efforts to develop software that would enable "no code" software development. Under the cease and desist order, the SPRK tokens are considered securities per *Howey* because the offering created a reasonable expectation of future profits based on Sparkster's managerial and entrepreneurial efforts.

So far in 2023, the SEC has continued its aggressive enforcement actions in this space—even in the absence of allegations of fraud—and has increasingly focused on crypto exchanges and other entities that facilitate crypto transactions:

- On January 12, 2023, the SEC charged Genesis Global Capital and Gemini Trust Company for "the unregistered offer and sale of securities to retail investors through the Gemini Earn crypto asset lending program."[149] The SEC alleged that Genesis "entered into an agreement with Gemini to offer Gemini customers, including retail investors in the United States, an opportunity to loan their crypto assets to Genesis in exchange for Genesis' promise to pay interest," and that in February 2021 Genesis and Gemini "began offering the Gemini Earn program to retail investors, whereby Gemini Earn investors tendered their crypto assets to Genesis, with Gemini acting as the agent to facilitate the transaction." The SEC further alleged that "Gemini deducted an agent fee, sometimes as high as 4.29 percent, from the returns Genesis paid to Gemini Earn investors" and that "Genesis then exercised its discretion in how to use investors' crypto assets to generate revenue and pay interest to Gemini Earn investors."
- On January 19, 2023, the SEC charged Nexo Capital with "failing to register the offer and sale of its retail crypto asset lending product, the Earn Interest Product (EIP)."[150] In a settlement, Nexo

[145] Complaint, *SEC v. Ripple Labs, Inc.*, No. 1:20-cv-10832 (S.D.N.Y. Dec. 22, 2020).
[146] Defendants' Memorandum of Law in Support of Their Motion for Summary Judgment, *SEC v. Ripple Labs, Inc.*, No. 1:20-cv-10832 (S.D.N.Y. Sept. 13, 2022).
[147] *SEC v. Dragonchain, Inc.*, No. 2:22-cv-01145 (W.D. Wash. Aug. 16, 2022); *see also SEC v. Hydrogen Tech. Corp.*, No. 1:22-cv-08284-LAK (S.D.N.Y. Sept. 29, 2022); *SEC v. Chicago Crypto Cap., LLC*, No. 1:22-cv-04975 (N.D. Ill. Sept. 14, 2022).
[148] *In re Sparkster, Ltd.*, Release No. 11102 (Sept. 19, 2022).
[149] *SEC v. Genesis Glob. Cap., LLC*, No. 23-cv-00287 (S.D.N.Y. Jan. 12, 2023).
[150] *In re Nexo Capital Inc.*, Release No. 11149 (Jan. 19, 2023).



agreed to pay a "$22.5 million penalty and cease its unregistered offer and sale of the EIP to U.S. investors"—in addition to "$22.5 million in fines to settle similar charges by state regulatory authorities" in a parallel action, which is discussed below.

- On February 9, 2023, the SEC charged Payward Ventures, Inc. and Payward Trading Ltd. (both commonly known as Kraken) with "failing to register the offer and sale of their crypto asset staking-as-a-service program, whereby investors transfer crypto assets to Kraken for staking in exchange for advertised annual investment returns of as much as 21 percent."[151] To settle the SEC's charges, the two Kraken entities "agreed to immediately cease offering or selling securities through crypto asset staking services or staking programs" as well as to "pay $30 million in disgorgement, prejudgment interest, and civil penalties."
- On March 29, 2023, the SEC charged crypto asset trading platform beaxy.com and its executives for "failing to register as a national securities exchange, broker, and clearing agency."[152] The SEC also charged Artak Hamazaspyan (founder of the Beaxy Platform) and a company he controlled (Beaxy Digital, Ltd.) with "raising $8 million in an unregistered offering of the Beaxy token (BXY) and alleged that Hamazaspyan misappropriated at least $900,000 for personal use, including gambling." The SEC also charged "market makers operating on the Beaxy Platform as unregistered dealers."
- On April 17, 2023, the SEC charged crypto asset trading platform Bittrex and its co-founder and former CEO, William Shihara, for "operating an unregistered national securities exchange, broker, and clearing agency."[153] The SEC also charged Bittrex's foreign affiliate, Bittrex Global GmbH, with "failing to register as a national securities exchange in connection with its operation of a single shared order book along with Bittrex." The SEC alleged that Bittrex earned at least $1.3 billion in revenues from 2017 through 2022 by holding itself out as "a platform that facilitated buying and selling of crypto assets" that the SEC alleges "were offered and sold as securities" without registration.

Fraud Schemes

The SEC has also pursued enforcement actions for various types of traditional fraud schemes that involve cryptocurrency. These cases are more likely to involve charges against individuals, rather than the entities themselves. Arguably the most popular alleged fraud scheme thus far in this space involves FTX, in which the SEC charged Samuel Bankman-Fried with violations of 17(a) of the Securities Act of 1933 and Section 10(b) of the Securities Exchange Act of 1934 and Rule 10b-5 thereunder.[154] The complaint emphasized that Bankman-Fried raised more than $1.8 billion from investors at least in part due to them believing that FTX had "appropriate controls and risk management measures." Further, while Bankman-Fried held himself out as a responsible leader in the crypto community, he "improperly diverted customer assets to his privately-held crypto hedge fund, Alameda Research LLC . . . and then used those customer funds to make undisclosed venture investments, lavish real estate purchases, and large political donations." Similar charges have been brought against other individuals,[155] including against Nishad Singh, the former Co-Lead Engineer of FTX, in February 2023.[156] Additional examples of alleged crypto fraud schemes are outlined below.

Pump and Dump Schemes

In September 2022, the SEC filed a complaint in the Southern District of Florida against Arbitrade and Cryptobontix, and their principals, regarding crypto assets that the SEC alleges bore "the hallmarks of a classic pump and dump scheme."[157] According to the

[151] *SEC v. Payward Ventures, Inc.*, No. 23-cv-00588 (N.D. Cal. Feb. 9, 2023).
[152] *SEC v. Beaxy Digit., Ltd.*, No. 23-cv-01962 (N.D. Ill. Mar. 29, 2023).
[153] *SEC v. Bittrex, Inc.*, No. 23-cv-00580 (W.D. Wash. Apr. 17, 2023).
[154] *SEC v. Bankman-Fried*, 1:22-cv-10501 (S.D.N.Y. Dec. 13, 2022).
[155] *See, e.g.*, *SEC v. Rounsville*, No. 3:22-cv-02458-D (N.D. Tex. Nov. 3, 2022); *SEC v. Balina*, No. 1:22-cv-00950 (W.D. Tex. Sept. 19, 2022); *SEC v. Barksdale*, No. 1:22-cv-01933 (S.D.N.Y. Mar. 8, 2022).
[156] *SEC v. Singh*, No. 23-cv-01691 (S.D.N.Y. Feb. 28, 2023).
[157] *SEC v. Arbitrade Ltd.*, No. 1:22-cv-23171 (S.D. Fla. Sept. 30, 2022).

complaint, the companies used "false and misleading releases and [a] press conference" to generate demand for the crypto asset "Dignity" or "DIG," which was owned and controlled by both companies. For example, Arbitrade falsely stated it had acquired and receive title to $10 billion in gold bullion for purposes of backing each DIG token with $1.00 worth of gold. In February, entries of default were issued against Arbitrade and Cryptobontix,[158] and on April 4, 2023, the Court denied the principals' motions to dismiss for lack of subject matter jurisdiction and failing to state a claim.[159]

Insider Trading

In July 2022, the SEC brought its first ever cryptocurrency insider trading enforcement action against a former Coinbase product manager, his brother, and a friend. The SEC alleged that, from June 2021 through April 2022, the former product manager shared information regarding upcoming cryptocurrency listings with the pair ahead of public announcements.[160] (The DOJ brought a parallel criminal action, described above.) The SEC explained in its press release that the group "purchased at least 25 crypto assets, at least nine of which were securities."[161] Thus, the SEC was required to take the position that certain digital assets were securities in order to bring charges under Section 10(b) of the Exchange Act.

Pyramid and Ponzi Schemes

In 2022, the SEC also pursued several alleged crypto-based pyramid and Ponzi schemes. Many involved Bitcoin, but other schemes involved alleged fake crypto assets and/or companies. For example, in one case, the SEC alleged that a fraudulent Ponzi scheme collected more than 82,000 Bitcoin, valued at $295 million at the time, from more than 100,000 investors on the premise of making a profit from alleged crypto asset trading activities using a crypto asset trading bot.[162] Investors were allegedly told that the bot made "millions of microtransactions" every second that would allow them to receive daily minimum returns of 0.35 percent. In another case, the SEC alleged that a fake crypto asset pyramid scheme functioned under the guise of a company that sold memberships as investments in its trading and mining operations that would be used to generate returns.[163] The alleged pyramid scheme expanded through the fake company's referral program. A third alleged combined pyramid and Ponzi scheme that raised more than $300 million from millions of investors functioned on a website that allowed investors to enter into transactions via smart contracts that operated on the Ethereum, Tron, and Binance blockchains.[164] Allegedly, investors could earn profits by recruiting others into the scheme, and assets from new investors were used to pay earlier investors.

On March 6, 2023, the SEC announced that it filed an emergency action and successfully obtained an asset freeze and appointment of a receiver against Miami-based investment adviser BKCoin Management LLC and one of its principals, Kevin Kang, "in connection with a crypto asset fraud scheme."[165] The SEC alleged that BKCoin and Kang "assured investors that their money would be used primarily to trade crypto assets and represented that BKCoin would generate returns for investors through separately managed accounts and five private funds," but then "disregarded the structure of the funds, commingled investor assets, and used more than $3.6 million to make Ponzi-like payments to fund investors."

Other Frauds

On January 20, 2023, the SEC charged Avraham Eisenberg with "orchestrating an attack on a crypto asset trading platform, Mango Markets, by manipulating the MNGO token, a so-called

---

[158] Entries of Default as to Arbitrade Ltd. and Cryptobontix Inc., *SEC v. Arbitrade Ltd.*, No. 1:22-cv-23171 (S.D. Fla. Feb. 14, 2023).
[159] Order on Motions to Dismiss, *SEC v. Arbitrade Ltd.*, No. 1:22-cv-23171 (S.D. Fla. Apr. 4, 2023).
[160] *SEC v. Wahi*, 2:22-cv-01009 (W.D. Wash. July 21, 2022). As noted above, the U.S. Attorney's Office for the Southern District of New York brought criminal charges against all three individuals.
[161] Press Release, Sec. & Exch. Comm'n, SEC Charges Former Coinbase Manager, Two Others in Crypto Asset Insider Trading Action (July 21, 2022), https://www.sec.gov/news/press-release/2022-127. Digital assets named in the enforcement action include POWR, AMP, RLY, DDX, XYO, RGT, LCX, DFX, and KROM.
[162] *SEC v. Braga*, 2:22-cv-01563 (W.D. Wash. Nov. 3, 2022).
[163] *SEC v. Da Silva*, 2:22-cv-10534 (S.D.N.Y. Dec. 14, 2022); *see also SEC v. Chavez*, 4:22-cv-03359 (S.D. Tex. Sept. 19, 2022) (finding that, rather than using investor funds to purchase and trade crypto or foreign exchange assets, Chavez "misappropriated the majority of investor money to fund his unrelated real estate company and his extravagant lifestyle").
[164] *SEC v. Okhotnikov*, 1:22-cv-03978 (E.D. Ill. Aug. 1, 2022).
[165] *SEC v. BKCoin Mgmt., LLC*, 1:23-cv-20719-RNS (S.D. Fla. Feb. 23, 2023).

governance token that was offered and sold as a security."[166] The SEC alleged that Eisenberg "engaged in a scheme to steal approximately $116 million worth of crypto assets from the Mango Markets platform" by using an account "he controlled on Mango Markets to sell a large amount of perpetual futures for MNGO tokens" and using "a separate account on Mango Markets to purchase those same perpetual futures."

On February 16, 2023, the SEC charged Singapore-based Terraform Labs and Do Hyeong Kwon with "orchestrating a multi-billion dollar crypto asset securities fraud involving an algorithmic stablecoin and other crypto asset securities."[167] The SEC alleged that Terraform and Kwon "raised billions of dollars from investors by offering and selling an inter-connected suite of crypto asset securities, many in unregistered transactions." These included "'mAssets,' security-based swaps designed to pay returns by mirroring the price of stocks of US companies," as well as Terra USD (UST), an alleged crypto asset security "referred to as an 'algorithmic stablecoin'" that Terraform designed to maintain "its peg to the U.S. dollar by being interchangeable for another of the defendants' crypto asset securities, LUNA." The SEC further alleged that Terraform and Kwon "offered and sold investors other means to invest in their crypto empire, including the crypto asset security tokens MIR—or 'mirror' tokens—and LUNA itself."

On March 22, 2023, the SEC charged numerous individuals and companies for the offer of unregistered securities, market manipulation, *and* touting.[168] Specifically, the SEC charged crypto asset entrepreneur Justin Sun and three of his wholly-owned companies, Tron Foundation Limited, BitTorrent Foundation Ltd., and Rainberry Inc. (formerly BitTorrent), for the "unregistered offer and sale of crypto asset securities Tronix (TRX) and BitTorrent (BTT)," for "fraudulently manipulating the secondary market for TRX through extensive wash trading," and "for orchestrating a scheme to pay celebrities to tout TRX and BTT without disclosing their compensation." The SEC also charged eight celebrities—including actress Lindsay Lohan, boxer Jake Paul, and several musical artists—for illegally touting TRX and/or BTT without disclosing that they were compensated and the amount of their compensation. All eight celebrities settled with the SEC.[169] In total, the SEC alleged that Sun generated proceeds of $31 million from illegal, unregistered offers and sales of the token.

Touting

Section 17(b) of the Securities Act makes it unlawful to promote a security without fully disclosing the receipt and amount of consideration from an issuer. And, as noted in the TRX and BTT charges described above, the SEC is focused on celebrities who allegedly tout unregistered securities. For example, in October 2022, Kim Kardashian settled with the SEC for touting EMAX tokens, which the SEC alleged to be "crypto asset securit[ies]."[170] To support this determination, the SEC cited in its order the DAO Report of Investigation from July 25, 2017, and the Commission's November 1, 2017, statement regarding celebrity promotions of cryptocurrency.[171] The cease and desist order stated that Kardashian promoted the EMAX token on her Instagram page in exchange for $250,000.

Similarly, on February 17, 2023, the SEC announced charges against former NBA star Paul Pierce for also touting EMAX tokens on social media "without disclosing the payment he received for the promotion and for making false and misleading promotional statements about the same crypto asset."[172] After failing to disclose that he was paid more than $244,000, Pierce agreed to settle the charges and pay $1.409 million "in penalties, disgorgement, and interest."

---

[166] *SEC v. Eisenberg*, No. 1:23-cv-00503 (S.D.N.Y. Jan. 20, 2023).
[167] *SEC v. Terraform Labs PTE Ltd.*, No. 1:23-cv-01346 (S.D.N.Y. Feb. 16, 2023).
[168] *SEC v. Sun*, No. 1:23-cv-02433 (S.D.N.Y. Mar. 22, 2023).
[169] *See In re Lohan*, Release No. 11173 (Mar. 22, 2023); *In re Mason*, Release No. 11174 (Mar. 22, 2023); *In re McCollum*, Release No. 11175 (Mar. 22, 2023); *In re Paul*, Release No. 11171 (Mar. 22, 2023); *In re Smith*, Release No. 11170 (Mar. 22, 2023); *In re Thiam*, Release No. 11172 (Mar. 22, 2023).
[170] *In re Kardashian*, Release No. 11116 (Oct. 3, 2022).
[171] Sec. & Exch. Comm'n, Report of Investigation Pursuant to Section 21(a) of the Securities Exchange Act of 1934: The DAO, Exchange Act Release No. 81207 (July 25, 2017), https://www.sec.gov/litigation/investreport/34-81207.pdf; Sec. & Exch. Comm'n, SEC Staff Statement Urging Caution Around Celebrity Backed ICOs (Nov. 1, 2017), https://www.sec.gov/news/public-statement/statement-potentially-unlawful-promotion-icos.
[172] *In re Pierce*, Release No. 11157 (Feb. 17, 2023).

Recent SEC Guidance

During the SEC Speaks 2022 conference, Chair Gensler stated that "[o]f nearly 10,000 tokens in the crypto market . . . the vast majority are securities."[173] More recently, Chair Gensler has built on this, articulating a view that the SEC has been clear in its guidance that almost all digital assets are securities. As noted above, Chair Gensler asserted in his prepared remarks in April 2023 to the House Financial Services Committee that Congress "gave the Commission a mandate to protect investors, regardless of the labels or technology used" and that "[n]othing about the crypto markets is incompatible with the securities laws."[174] In his view, "the vast majority of crypto tokens are securities" as "[t]he investing public generally is buying crypto tokens because those investors are anticipating a profit and hoping for a better future" based, at least in part, on the support of "websites and social media accounts" and "entrepreneurs backing them." "Given that most crypto tokens are securities, it follows that many crypto intermediaries are transacting in securities and have to register with the SEC," said Chair Gensler.

Chair Gensler also stated that the "market is rife with noncompliance," which "puts investors at risk" as well as "the public's trust in our capital markets."[175] To this end, he noted the SEC is "the cop on the beat watching out for [the Committee Members'] constituents" and has, in the last two years, "filed nearly 1,500 enforcement actions and conducted more than 6,000 examinations of registrants." In his view, "[c]rypto intermediaries—whether they call themselves centralized or decentralized—often provide an amalgam of services that typically are separated from each other in the rest of the securities markets: exchange functions, broker-dealer functions, custodial and clearing functions, and lending functions," and thus the "commingling of the various functions within crypto intermediaries creates inherent conflicts of interest and risks for investors," which are "risks and conflicts the Commission does not allow in any other marketplace." "It's the law; it's not a choice. Calling yourself a DeFi platform, for instance, is not an excuse to defy the securities laws," asserted Chair Gensler.

In closing, Chair Gensler explained that the Commission has "spoken directly to crypto market participants in enforcement actions and a number of rule proposals," and he reiterated his belief that the best execution rule (proposed in December 2022) would "cover all crypto assets."[176]

Members of the Committee challenged Chair Gensler's approach. Rep. McHenry called the SEC's approach "regulation by enforcement" and stated the SEC is "punishing digital-asset firms for allegedly not adhering to the law when they don't know it will apply to them."[177]

Kristin Smith, CEO of the Blockchain Association, also characterized Chair Gensler's testimony as reflecting "the SEC's approach to the crypto economy: confusing, unclear, opaque, and ultimately blind to the harm its regulation by enforcement strategy is doing to lawful companies in this country."

But Rep. Stephen Lunch (D – Mass.) expressed similar sentiment to Chair Gensler, noting "[t]here is a fair amount of guidance out there and clarity; it's just not the clarity that the crypto industry wants." Notably, Chair Gensler refused multiple queries by Rep. McHenry as to whether ether is a security. Instead, he repeatedly answered that "it depends on the facts and the law."[178]

Prior to Chair Gensler's testimony, the House Financial Services Committee expressed concerns about the SEC's regulatory approach. Specifically, the Committee said the SEC had "forced digital asset

[173] Gary Gensler, Sec. & Exch. Comm'n, Kennedy and Crypto (Sept. 8, 2022), https://www.sec.gov/news/speech/gensler-sec-speaks-090822.
[174] Gary Gensler, Chair, Sec. & Exch. Comm'n, Testimony of Chair Gary Gensler Before the United States House of Representatives Committee on Financial Services (Apr. 18, 2023), https://www.sec.gov/news/testimony/gensler-testimony-house-financial-services-041823.
[175] *Id.*
[176] *Id.*
[177] Paul Kiernan, *Republicans Pummel SEC's Gary Gensler Over Crypto Crackdown*, WALL ST. J. (Apr. 18, 2023), https://www.wsj.com/articles/sec-chair-gensler-to-defend-climate-crypto-plans-before-gop-led-panel-2e3a6ade.
[178] Nikhilesh De, *SEC Chair Gensler Declines to Say if Ether Is a Security in Contentious Congressional Hearing*, COINDESK (Apr. 19, 2023), https://www.coindesk.com/policy/2023/04/19/sec-chair-gensler-declines-to-say-if-ether-is-a-security-in-contentious-congressional-hearing/.

market participants into regulatory frameworks that are neither compatible with the underlying technology nor applicable because the firms' activities do not involve an offering of securities," and that these "approaches hamper the digital asset ecosystem's ability to realize the unique benefits the new technology offers, which harms consumers, investors, and the economy as a whole."[179]

SEC Commissioner Mark Uyeda has expressed that regulation by enforcement "fails to provide the nuanced and comprehensive guidance that allows market participants to tailor their practices."[180] Such thoughts are shared by other commissioners like Hester Peirce, an outspoken critic of the SEC's approach and so-called "Crypto Mom." One of her key focus areas is on the hurdles crypto companies face to go through the lengthy and complex process of registering their products with the SEC.[181]

[179] Letter from Comm. on Fin. Servs., U.S. House of Representatives, to Gary Gensler, Chair, Sec. & Exch. Comm'n (Apr. 18, 2023), https://financialservices.house.gov/uploadedfiles/2023-04-17_all_fsc_gop_letter_to_sec_on_nse_registration_final.pdf.
[180] Mark T. Uyeda, Sec. & Exch. Comm'n, Remarks at the "SEC Speaks" Conference 2022 (Sept. 9, 2022), https://www.sec.gov/news/speech/uyeda-speech-sec-speaks-090922.
[181] *See, e.g.*, Hester M. Peirce, Sec. & Exch. Comm'n, Statement on Settlement with BlockFi Lending LLC (Feb. 14, 2022), https://www.sec.gov/news/statement/peirce-blockfi-20220214.

Financial Crimes Enforcement Network

Introduction

The U.S. Department of the Treasury's ("Treasury") Financial Crimes Enforcement Network ("FinCEN") was established to safeguard the financial system from illicit use, combat money laundering and its related crimes, including terrorism, and promote national security through the strategic use of financial authorities and the collection, analysis, and dissemination of financial intelligence.

FinCEN's anti-money laundering compliance expectations for U.S.-based cryptocurrency companies have grown in recent years, mainly due to the fact that cryptocurrencies are being used at a much larger scale for transactions and as payment for services. Since 2013, guidance from FinCEN has clarified that operators of cryptocurrency exchanges should be treated as money transmitters and therefore are required to follow Bank Secrecy Act ("BSA") regulations that apply to banks and other financial institutions.[182] In 2013, FinCEN issued guidance that clarified the applicability of the BSA to transactions involving the transmission of convertible virtual currency.[183] In 2019, FinCEN issued further guidance providing that whether a person qualifies as a money service business subject to BSA regulation depends on the person's activities and not its formal business status.[184]

Broadly stated, cryptocurrency exchanges are money services businesses ("MSBs") on the basis that cryptocurrency tokens are "other value that substitutes for currency." Section 6102(d) of the Anti-Money Laundering Act of 2020 ("AMLA") expanded the definition of "financial institutions" to include businesses involved in the exchange of "value that substitutes for currency or funds," thus codifying FinCEN's longstanding position that cryptocurrency exchanges—which convert fiat currency such as the U.S. dollar into cryptocurrency and vice versa—are "money services businesses" subject to BSA reporting requirements.

This requires cryptocurrency exchanges to engage in customer due diligence ("CDD") to verify the identity of their customers, identify any beneficial owners of accounts, develop customer risk profiles, and monitor transactions to submit suspicious activity reports ("SARs"), among other requirements.[185]

In response to guidelines published in June 2019 by the Financial Action Task Force ("FATF"), an inter-governmental body that sets policy aimed at combating money laundering and financing of terrorism,[186] FinCEN made clear that it expects cryptocurrency exchanges to comply with the so-called "Travel Rule," which requires financial institutions to gather information about the originators and beneficiaries of transactions and share that information down the payment chain to any receiving financial institution. FinCEN's application of the Travel Rule to cryptocurrency exchanges places such exchanges in the same regulatory category as traditional money transmitters and applies the same regulations, including those set out in the BSA. In 2020, FinCEN released a Notice of Proposed

[182] The Financial Recordkeeping and Reporting of Currency and Foreign Transactions Reporting Act of 1970 ("Bank Secrecy Act"), 31 U.S.C. § 5311 *et seq*.
[183] FinCEN, U.S. Dep't of Treasury, Application of FinCEN's Regulations to Persons Administering, Exchanging, or Using Virtual Currencies (March 2013), https://www.fincen.gov/sites/default/files/shared/FIN-2013-G001.pdf.
[184] FinCEN, U.S. Dep't of Treasury, Application of FinCEN's Regulations to Certain Business Models Involving Convertible Virtual Currencies 3 (May 2019), https://www.fincen.gov/sites/default/files/2019-05/FinCEN%20Guidance%20CVC%20FINAL%20508.pdf.
[185] *See* 31 C.F.R. § 1010.
[186] *See* FATF, Guidance for a Risk-Based Approach, Virtual Assets and Virtual Asset Service Providers (June 2019).

Rulemaking ("NPRM") on modifications to the Travel Rule, which signaled the introduction of new compliance responsibilities for cryptocurrency exchanges.[187]

Significant Publications, Speeches, and Enforcement Actions in 2022

On September 16, 2022, Treasury published three reports pursuant to Sections 4, 5, and 7 of President Joe Biden's Executive Order 14067 on "Ensuring Responsible Development of Digital Assets," which calls for an alignment of the federal government's approach to digital assets. Those reports contain recommendations for policymakers on how to minimize the risks of digital assets, including but not limited to, money laundering and terrorist financing.[188] The reports have the same overarching message—Treasury plans on exercising greater oversight of the digital asset industry.

"Action Plan to Address Illicit Financing Risks of Digital Assets"

One of the three reports is an "Action Plan to Address Illicit Financing Risks of Digital Assets" (the "Action Plan"), intended as a plan for mitigating digital asset-related illicit finance and national security risks. The Action Plan begins by identifying several aspects of digital assets that present opportunities for misuse by illicit actors. First, given gaps in the anti-money laundering regimes across countries, illicit actors select virtual asset service providers ("VASPs") that operate out of jurisdictions with minimal anti-money laundering and counter-financing of terrorism ("AML/CFT") requirements.[189]

Second, the Action Plan discusses the presence of anonymity-enhancing technologies, such as enhanced cryptography, operation on an opaque blockchain, and anonymizing services that can obscure transactional activity and limit transparency.[190] Certain anonymizing services, such as mixers and tumblers, accept virtual assets and retransmit them in a manner that masks the original source of the asset, thereby concealing the movement and origin of funds—making those services popular among illicit actors.[191] For example, ransomware cybercriminals typically use mixers and tumblers to receive and launder their illicit proceeds.[192]

Third, disintermediated assets that are transferred and self-custodied without the involvement of a financial institution also pose money laundering risks.[193] U.S. law enforcement agencies have seen a trend in the use of peer-to-peer ("P2P") transactions—transfers of virtual assets via wallets not hosted by any financial institutions or VASPs—to evade money laundering regulations.[194] The Action Plan stresses that, depending on the business model, P2P service providers are subject to AML/CFT obligations as money service businesses.[195]

Although not mentioned in the Action Plan, U.S. enforcement authorities are also monitoring the market for NFTs, which (as noted above) are digital units on the underlying blockchain that represent ownership of media or of physical or digital property.[196] NFTs that are used in practice as collectibles are generally not considered virtual assets.[197] However, NFTs that are used for payment or investment purposes or NFT platforms that allow owners to sell digital art on virtual exchanges may be considered virtual assets and be subject to AML/CFT obligations.[198] Like other disintermediated assets, NFTs can be traded via P2P transactions without an intermediary. This feature can be misused by

---

[187] Pilot Program on Sharing of Suspicious Activity Reports and Related Information with Foreign Branches, Subsidiaries, and Affiliates, 87 Fed. Reg. 3719 (proposed Jan. 25, 2022) (to be codified at 31 C.F.R. pt. 1010), https://www.federalregister.gov/documents/2022/01/25/2022-01331/pilot-program-on-sharing-of-suspicious-activity-reports-and-related-information-with-foreign.

[188] Press Release, U.S. Dep't of Treasury, Statement from Secretary of the Treasury Janet L. Yellen on the Release of Reports on Digital Assets (Sept. 16, 2022), https://home.treasury.gov/news/press-releases/jy0956.

[189] U.S. Dep't of Treasury, Action Plan to Address Illicit Financing Risks of Digital Assets 4–5 (Sept. 2022).

[190] *Id.* at 5.

[191] *Id.*

[192] FATF, Targeted Updated on Implementation of the FATF Standards on Virtual Assets and Virtual Asset Service Providers 22 (June 2022).

[193] U.S. Dep't of Treasury, *supra* note 189, at 5.

[194] *Id.*; *see also* U.S. Dep't of Treasury, National Money Laundering Risk Assessment 45 (Feb. 2022).

[195] U.S. Dep't of Treasury, *supra* note 189, at 6.

[196] U.S. Dep't of Treasury, Study of the Facilitation of Money Laundering and Terror Finance Through the Trade in Works of Art 25 (Feb. 2022).

[197] *Id.* at 26.

[198] *Id.*

criminals who use NFTs for illicit financial activity, such as money laundering and wash trading.[199]

U.S. law enforcement investigations are also focused on Decentralized Finance ("DeFi") services, which are virtual asset platforms that allow for P2P transactions through smart contracts, without the need for an account or custodial relationship (or regulated financial intermediaries subject to the BSA).[200] DeFi services are attractive to criminals as they often involve no AML/CFT or other processes to identify customers or suspicious activity. The Action Plan warns that if DeFi services are run through a decentralized autonomous organization or concentrated ownership that accepts and transmits currency or funds, they may be operating as a money transmitter and will be subject to AML/CFT requirements.[201] Thus, businesses that offer services involving DeFis, NFTs, and unhosted wallets must conduct a careful analysis of their structure and their specific activities to determine whether they are subject to AML/CFT obligations.

Treasury has outlined the priority actions that the U.S. should take to address the vulnerabilities and emerging risks associated with digital assets and their misuse. One of the priorities is to update or modernize the BSA regulations to account for these emerging risks. FinCEN has committed to closely monitoring emerging financial technologies and assessing whether they warrant new regulations and whether gaps exist in the AML/CFT framework.[202] In line with that priority, FinCEN is considering adjustments to the Recordkeeping Rule and the Travel Rule.[203] Currently, the Recordkeeping Rule requires financial institutions to collect and retain information on certain fund transfers of $3,000 or more.[204] FinCEN's Travel Rule requires financial institutions to transmit to other financial institutions in the payment chain the information on certain funds transfers of $3,000 or more.[205] Such information includes: transmitter's name, account number, address, identity of the recipient's financial institutions, transmitter's payment instructions, amount, and date of transfer. If the funds are received, the financial institution must also retain the recipient's name, address, account number, and other specific identifiers.[206]

In 2019, FinCEN expanded the Travel Rule to apply to virtual currency businesses.[207] In October 2020, FinCEN proposed lowering the $3,000 threshold requirement to $250 for international transactions.[208] Now, as part of the Action Plan, FinCEN is once again considering lowering the $3,000 threshold requirement to "collect, retain, and transmit [information] to other financial institutions."[209]

FinCEN also proposed a new rule to impose data collection requirements on cryptocurrency exchanges and wallets. The rule, which was expected to be implemented in August 2022, would require exchanges to submit reports with FinCEN[210] for transactions over $10,000 whenever customers transact with a counterparty whose wallet is either unhosted or held by a financial institution in certain foreign jurisdictions (an "otherwise covered wallet"), and recordkeeping of transactions involving the sending of $3,000 or more to "unhosted wallets."[211] Another priority of Treasury is "to strengthen U.S.

---

[199] *Id.* at 27; *see also* FATF, *supra* note 192, at 20 ("Wash trading refers to executing a transaction in which the seller is on both sides of the trade in order to paint a misleading picture of an asset's value and liquidity.").
[200] U.S. DEP'T OF TREASURY, *supra* note 189, at 6.
[201] *Id.* at 7.
[202] *Id.* at 12.
[203] In 1995, FinCEN published final regulations requiring "financial institutions other than depository institutions," including securities brokers and money transmission services, to report on international transfers of funds of $3,000 or more (known generally as the Record Keeping and Travel Rules).
[204] 31 CFR § 1020.410(a); 31 CFR § 1010.410(a).
[205] 31 CFR § 1010.410(f).
[206] *Id.*
[207] FINCEN, APPLICATION OF FINCEN'S REGULATIONS TO CERTAIN BUSINESS MODELS INVOLVING CONVERTIBLE VIRTUAL CURRENCIES (May 9, 2019), https://www.fincen.gov/sites/default/files/201905/FinCEN%20Guidance%20CVC%20FINAL%20508.pdf.
[208] Semiannual Agenda and Regulatory Plan, 87 Fed. Reg. 5278, 5281 (proposed Jan. 31, 2022), https://www.federalregister.gov/documents/2022/01/31/2021-27949/semiannual-agenda-and-regulatory-plan.
[209] U.S. DEP'T OF TREASURY, *supra* note 189, at 12–13.
[210] The report must contain certain customer and counterparty information such as identification, physical address, taxpayer identification numbers, and identity verification documents, cross-referenced to existing currency transaction report information requirements ("CTRs").
[211] *See* Requirements for Certain Transactions Involving Convertible Virtual Currency or Digital Assets, 85 Fed. Reg. 83840 (proposed Dec. 23, 2020) (to be codified at 31 C.F.R. pts. 1010, 1020, 1022), https://www.federalregister.gov/documents/2020/12/23/2020-28437/requirements-for-certain-transactions-involving-convertible-virtual-currency-or-digital-assets. For purposes of

AML/CFT supervision of virtual asset activities, which includes standardization of AML/CFT obligations across states, making sure that VASPs that do business, wholly or substantially, in the U.S. register with relevant authorities and implement AML/CFT requirements, and pursue enforcement actions against VASPs that fail to do so."[212] As part of this priority,

Treasury will "strengthen FinCEN's existing supervisory enforcement function to increase and harmonize compliance with AML/CFT requirements, especially through examinations and related compliance and enforcement investigations and actions."[213]

The law enforcement agencies will closely monitor "mixing services, darknet markets, and non-compliant VASPs used to launder or cash out illicit funds" as well as VASPs that process ransomware-related payments.[214] Treasury advises that those who are involved in such illicit activity could be sanctioned, and therefore cut off from the international financial system.[215]

Treasury's other priority is to engage with the private sector to ensure that it understands existing obligations and illicit financing risks. As part of that effort, FinCEN is considering expanding its Section 314(a) program to include more VASPs.[216] Section 314(a) of the U.S. Patriot Act enables Treasury to reach out to financial institutions to locate accounts and transactions of persons identified by law enforcement that may be involved in terrorism or money laundering.[217] Several VASPs are already subject to the information sharing requirements set forth under Section 314(a). Treasury believes that expanding this program to include more VASPs will allow for further engagement with the private sector and enhance law enforcement efforts to identify illicit actors.[218]

For the past few years, the U.S. Government has been actively working with FATF and other international bodies to promote effective regulation, supervision, and enforcement related to virtual assets.[219] It is Treasury's priority to continue its work with FATF to encourage and support the implementation of FATF standards for virtual assets globally—such as the application of the Travel Rule, which is similar to FinCEN's Travel Rule but mandates a lower threshold of $1,000.[220] As part of Treasury's priority to improve global AML/CFT regulation and enforcement, it plans on sharing information with partners to support international prosecution of the abuse of digital assets.[221]

The Report on "Crypto-Assets: Implications for Consumers, Investors, and Businesses"

Another one of the three reports published by Treasury this past September, titled "Crypto-Assets: Implications for Consumers, Investors, and Businesses," analyzed the current opportunities and risks in the crypto-assets ecosystem and their implications for consumers, investors, and businesses. Treasury noted that risks arise particularly from "non-compliance with (i) the extensive disclosure requirements for registered exchanges, products, and intermediaries that are designed to provide investors and customers with material and relevant information and (ii) the requirements around market conduct that are designed to provide fair, orderly, and efficient markets."[222]

The report laid out recommendations to address the risk of digital assets. The first recommendation advises U.S. regulatory and law enforcement authorities to "pursue vigilant monitoring of the crypto-asset sector for unlawful activity, aggressively pursue investigations, and bring civil and criminal actions to

---

the NPRM, a "hosted wallet" is one where an owner's private keys are held by a regulated financial institution. An "unhosted wallet" is one where the private keys are not held by a regulated financial institution, also often referred to as a "self-hosted" wallet.

[212] U.S. DEP'T OF TREASURY, *supra* note 189, at 13.

[213] *Id.*

[214] *Id.* at 14.

[215] *Id.*

[216] *Id.* at 15.

[217] 31 CFR § 1010.520; *see* FINCEN, FINCEN'S 314(A) FACT SHEET (Nov. 29, 2022), https://www.fincen.gov/sites/default/files/shared/314afactsheet.pdf.

[218] U.S. DEP'T OF TREASURY, *supra* note 189, at 15.

[219] *Id.* at 11.

[220] *Id.*

[221] *Id.* at 12.

[222] U.S. DEP'T OF TREASURY, CRYPTO-ASSETS: IMPLICATIONS FOR CONSUMERS, INVESTORS, AND BUSINESSES 40 (Sept. 2022).

enforce applicable laws with a particular focus on consumer, investor, and market protection."[223] The report called for increased investigations into "misrepresentations made to consumers and investors in crypto-assets, including, for example, false or misleading advertising, terms of service, claims of returns or income potential, or statements of protections available to users of crypto-assets," crypto-assets sold as collectibles or as features of gaming and entertainment, and crypto-assets marketed as retirement plans.[224] The Secretary of the Treasury Janet Yellen later echoed the report's emphasis on vigilant monitoring during her statement on recent crypto market developments where she emphasized "the need for more effective oversight of cryptocurrency markets." Yellen called for "rigorous" enforcement of investor and consumer protection laws that apply to crypto assets and services and called for Congress to "move quickly to fill the regulatory" gaps in the crypto sphere.[225]

The other recommendations in the report advised U.S. regulatory agencies to continue issuing supervisory guidance and rules to address emerging risks in crypto-asset products and services which means that further rulemaking related to crypto-assets is expected.

The Report on "The Future of Money and Payments"

The last of Treasury's publications was a report on "The Future of Money and Payments," which analyzed how the potential creation of a U.S. Central Bank Digital Currency ("CBDC"), instant payment systems, and stablecoins may impact U.S. money and payment systems and AML/CFT obligations. When discussing stablecoins in particular, the report acknowledged the risks of a poorly designed and inadequately regulated stablecoin and noted that "if a stablecoin was widely adopted globally as a means of payment, the stablecoin could pose greater risks for illicit finance due to uneven implementation of global AML/CFT standards for digital assets."[226] According to the report,

> *"[t]he liquidity of a widely adopted stablecoin could also make it attractive to criminals and the design of a stablecoin arrangement (e.g., use of permissioned blockchain) could affect the implementation of AML/CFT requirements."*[227]

The report called for regulation and oversight of stablecoins to address their risk to the financial system, consumers, and investors.[228] Thus, the U.S. Government is likely to issue further guidance or rules regulating stablecoins.

FinCEN's 2022 Speeches on Digital Identity and Responsible Innovation

In 2022, FinCEN's representatives gave multiple speeches that can serve to frame FinCEN's priorities in the crypto space. On May 19, 2022, FinCEN's Associate Director of the Enforcement and Compliance Division, Alessio Evangelista, spoke at the Chainalysis Links Conference on "The Intersection of Cryptocurrencies and National Security."[229] Evangelista introduced FinCEN's approach to the crypto space as that of "responsible financial innovation,"[230] meaning "financial institutions that operate in the cryptocurrency space have the same obligations as all other financial institutions to ensure that their new offerings can leverage innovations while still protecting consumers, reducing cybercrime, combating illicit financial activity, and ensuring their platforms are not used to harm national security interests."[231] Evangelista's examples of responsible innovations included "innovative Travel

---

[223] *Id.* at 50.
[224] *Id.* at 50–51.
[225] Press Release, U.S. Dep't of Treasury, Statement by Secretary of the Treasury Janet L. Yellen on Recent Crypto Market Developments (Nov. 16, 2022), https://home.treasury.gov/news/press-releases/jy1111.
[226] U.S. DEP'T OF TREASURY, THE FUTURE OF MONEY AND PAYMENTS 18 (Sept. 2022).
[227] *Id.* at 17–18.
[228] *Id.* at 17.
[229] FinCEN, Prepared Remarks of Alessio Evangelista, Associate Director, Enforcement and Compliance Division, During Chainalysis Links Conference (May 19, 2022), https://www.fincen.gov/news/speeches/prepared-remarks-alessio-evangelista-associate-director-enforcement-and-compliance.
[230] Janet Yellen echoed Evangelista in her April 7, 2022, speech to the American University's Kogod School of Business Center for Innovation where she spoke on the importance of "responsible innovation" that protects national security interests and the planet. U.S. Dep't of Treasury, Remarks from Secretary of the Treasury Janet L. Yellen on Digital Assets (Apr. 7, 2022), https://home.treasury.gov/news/press-releases/jy0706.
[231] FinCEN, *supra* note 229.

Rule solutions, geo-blocking capabilities, the development of protocols that embed Customer Due Diligence[,] and sanctions screening."[232] Evangelista commented that cryptocurrency companies must have strong compliance policies, make informed risk-based decisions, and file SARs.[233] Evangelista emphasized that "addressing the illicit finance and national security risks related to Travel Rule compliance and unhosted wallets" remains FinCEN's priority.[234]

On April 4, 2022, FinCEN's Acting Director Himamauli Das spoke at FDIC-FinCEN Digital Identity Tech Sprint Demonstration Day.[235] FinCEN's Acting Deputy Director Jimmy Kirby spoke during the 2022 Federal Identity Forum & Exposition and the January 2023 Identity Policy Forum.[236] Both speeches emphasized FinCEN's focus on identity-related crimes, including fraud and cyber events. FinCEN's officials expressed concern about the "increase in potential identity verification, impersonation, and compromise-related suspicious activity."[237] For example, SARs filers reported that they were unable to recognize fraudulent identities at the time of transactions due to insufficient identity verification processes.[238] Both officials called for strengthened regulations and reporting requirements to combat identity-related crimes. Those speeches should serve as a message to crypto-asset trading platforms that FinCEN will monitor their customer identification and verification processes and their ability to detect, investigate, and report transactions connected to illicit activity.

FinCEN's Enforcement Action Against Bittrex, Inc.

Last year, FinCEN, along with Treasury's Office of Foreign Assets Control ("OFAC"), pursued the first joint action against a convertible virtual currency trading platform, Bittrex, Inc. ("Bittrex"). On October 11, 2022, FinCEN announced a $29,280,829.20 settlement against Bittrex for violations of the BSA.[239] Specifically, FinCEN determined that Bittrex failed to develop, implement, and maintain an effective anti-money laundering program "that was reasonably designed to prevent its CVC [convertible virtual currency] trading platform and hosted wallet service from being used to facilitate money laundering and the financing of terrorist activities. Additionally, FinCEN determined that Bittrex failed to accurately, and timely, report suspicious transactions to FinCEN."[240]

FinCEN's investigation found that from February 2014 through October 2017, Bittrex relied on two employees to manually review all transactions for suspicious activity. As a result, Bittrex failed to detect suspicious transactions through its platform, including transactions with darknet marketplaces and transactions valued at over $260 million with entities and individuals located in sanctioned jurisdictions like Iran, Syria, and the Crimea region of Ukraine. Bittrex also did not file any SARs from 2014 to May 2017. FinCEN's investigation concluded that Bittrex failed to address the risk associated with anonymity-enhanced cryptocurrencies and to detect, investigate, and report transactions connected to ransomware attacks against individuals and small businesses in the United States. This settlement, in combination with FinCEN's BitMEX settlement in August 2021 for willfully failing to comply with its obligations under the BSA as part of a global settlement with the CFTC,[241] suggests that FinCEN will continue to pursue enforcement actions against crypto platforms and

---

[232] *Id.*
[233] Id.
[234] Id.
[235] FinCEN, Prepared Remarks of FinCEN Acting Director Himamauli Das During the FDIC-FinCEN Digital Identity Tech Sprint Demonstration Day (Apr. 8, 2022), https://www.fincen.gov/news/speeches/prepared-remarks-fincen-acting-director-himamauli-das-during-fdic-fincen-digital.
[236] FinCEN, Prepared Remarks of FinCEN Acting Deputy Director Jimmy Kirby During the 2022 Federal Identity Forum & Exposition (FedID) (Sept. 7, 2022), https://www.fincen.gov/news/speeches/prepared-remarks-fincen-acting-deputy-director-jimmy-kirby-during-2022-federal; FinCEN, Prepared Remarks of FinCEN Acting Deputy Director Jimmy Kirby During the Identity Policy Forum (Jan. 25, 2023), https://www.fincen.gov/news/speeches/prepared-remarks-fincen-acting-deputy-director-jimmy-kirby-during-identity-policy.
[237] Id.
[238] Id.
[239] Press Release, FinCEN, FinCEN Announces $29 Million Enforcement Action Against Virtual Asset Service Provider Bittrex for Willful Violations of the Bank Secrecy Act (Oct. 11, 2022), https://www.fincen.gov/news/news-releases/fincen-announces-29-million-enforcement-action-against-virtual-asset-service.
[240] In re Bittrex, Inc., No. 2022-03, at 10 (Oct. 11, 2022).
[241] Press Release, FinCEN, FinCEN Announces $100 Million Enforcement Action Against Unregistered Futures Commission Merchant BitMEX for Willful Violations of the Bank Secrecy Act (August 10, 2021), https://www.fincen.gov/news/news-releases/fincen-announces-100-million-enforcement-action-against-unregistered-futures.

exchanges that fail to comply with their AML/CFT obligations.

The NYDFS Settlements with Coinbase and Robinhood Crypto

As discussed more fully below, *infra* § X, on January 4, 2023, the New York State Department of Financial Services entered into a $50 million settlement agreement with Coinbase caused by significant failures in Coinbase's AML program.[242] As part of the settlement agreement, Coinbase agreed to invest another $50 million into a compliance program. NYDFS found that Coinbase had noncompliant Know Your Customer ("KYC") procedures, Transaction Monitoring System, and OFAC screening program such that "Coinbase treated customer onboarding requirements as simple check-the-box exercise and failed to conduct appropriate due diligence." Coinbase lacked sufficient personnel, resources, and tools needed to keep up with transactional monitoring alerts that resulted in a backlog of over 100,000 alerts.

This was not the first enforcement action by the NYDFS against crypto platforms. On August 2, 2022, the NYDFS entered into a $30 million settlement agreement with Robinhood Crypto ("RHC") as a result of its failure "to maintain an effective BSA/AML program, including an adequate transaction monitoring system, commensurate with its growth."[243] RHC's BSA/AML program was inadequately staffed, failed to timely transition from a manual transaction monitoring system that was inadequate for RHC's size, customer profiles, and transaction volumes, and did not devote sufficient resources to adequately address risks specific to RHC. As part of the settlement agreement, RHC was required to retain an independent consultant that will perform an evaluation of RHC's compliance. Those settlements show that the regulators will continue to pursue enforcement actions against platforms with noncompliant AML programs.

FinCEN Alert on Potential Sanctions Evasion Efforts

On March 7, 2022, FinCEN issued an alert regarding the evasion of sanctions implemented in connection with Russia's invasion of Ukraine. The alert warns that sanctioned persons, illicit actors, and their related networks or facilitators may attempt to use CVC to evade sanctions. The red flag indicators outlined by FinCEN include: (1) a customer's transactions involving Internet Protocol ("IP") addresses from non-trusted sources, locations in Russia, Belarus, or FATF-identified jurisdictions with AML/CFT and countering-proliferation deficiencies, and comprehensively sanctioned jurisdictions, as well as IP addresses previously flagged as suspicious; (2) transactions connected to CVC addresses listed on OFAC's Specially Designated Nationals and Blocked Persons List; and (3) transactions using a CVC exchanger or foreign-located money services business in a high-risk jurisdiction with AML/CFT deficiencies, inadequate or insufficient know-your-customer requirements, or CDD measures.[244] The alert encourages all U.S. financial institutions to voluntarily share information about sanctions evasion, ransomware/cyberattacks, money laundering, and proceeds of corruption or other malign activities related to Russia and Belarus, undertake appropriate risk-based due diligence of customers, and, where necessary, conduct enhanced due diligence.

The alert also reminds financial institutions of their obligations to file SARs, specifically noting that "institutions that perform CVC exchanges must identify and immediately report suspicious transactions associated with ransomware attacks."[245] This alert is part of Treasury's broader effort to

---

[242] New York State, Superintendent Adrienne A. Harris Announces $100 Million Settlement with Coinbase, Inc. after DFS Investigation Finds Significant Failings in the Company's Compliance Program (Jan. 4, 2023), https://www.dfs.ny.gov/reports_and_publications/press_releases/pr202301041; see Consent Order at https://www.dfs.ny.gov/system/files/documents/2023/01/ea20230104_coinbase.pdf.

[243] New York State, DFS Superintendent Harris Announces $30 Million Penalty on Robinhood Crypto For Significant Anti-Money Laundering, Cybersecurity & Consumer Protection Violations (Aug. 2, 2022), https://www.dfs.ny.gov/reports_and_publications/press_releases/pr202208021; see Consent Order at https://www.dfs.ny.gov/system/files/documents/2022/08/ea20220801_robinhood.pdf

[244] FinCEN, FinCEN Alert, 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.

[245] Id.

address sanctions evasions by certain Russian actors.

On January 18, 2023, FinCEN issued an order identifying a virtual currency exchange Bitzlato Limited as a "primary money laundering concern" in connection with Russian illicit finance and prohibiting certain transmittals of funds involving Bitzlato by any covered financial institution. This was the first order issued pursuant to section 9714(a) of the Combating Russian Money Laundering Act. Bitzlato played a critical role in laundering CVCs by facilitating illicit transactions for ransomware actors operating in Russia. This order is part of FinCEN's efforts to target Russian illicit financial activity and counter ransomware threats.[246]

Outlook for 2023

Treasury has emphasized an urgent need for greater crypto regulation to combat global and domestic criminal activities. Commenters on the reports issued pursuant to Executive Order 14067 on "Ensuring Responsible Development of Digital Assets" have generally echoed that view, noting both the lack of regulatory clarity in the digital assets industry, as well as lack of consensus regarding the risks involved given that some digital asset transactions involve more complexity and illicit finance risk than others.[247]

As discussed above, FinCEN has proposed cryptocurrency regulations to impose data collection and transmission requirements (*e.g.*, the Travel Rule) on cryptocurrency exchanges and digital wallets that it likely will either repropose for further comment or finalize in 2023. Among other things, the proposed rule would classify cryptocurrencies and central bank digital currencies, which are not yet in wide circulation, as "monetary instruments" for purposes of the BSA, which may trigger criminal penalties for conduct involving the structuring of virtual currency transactions to evade or avoid reporting requirements.

FinCEN's Digital Asset Plan provides that it will publish a risk assessment by February 24, 2023 on the money laundering and terrorist financing risks related to DeFi; the same plan also calls for the publication of a risk assessment by July 2023 on the money laundering and terrorist financing risks related to NFTs.[248] FinCEN also is likely to issue further guidance clarifying that DeFi exchanges that provide P2P services will be required to comply with BSA obligations that apply to money transmitters, including registering with FinCEN as a money service business and complying with BSA/AML requirements, such as filing SARs.

With the exception of NFTs in the high-value art market,[249] FinCEN has yet to issue anything specifically on NFTs; nor has it indicated that NFT exchanges are required to conduct compliance like money services businesses. NFT platforms should nonetheless assess their obligations to implement AML/CFT procedures based on FATF's "functional approach" to assessing various types of financial assets that an NFT may represent.[250] Given the high degree of scrutiny and ongoing expansion of AML obligations to the cryptocurrency area, we can expect additional guidance regarding NFTs this year.

As explained above, *supra* § III, on December 13, 2022, Senators Elizabeth Warren and Roger Marshall introduced the "DAAML Act" that is intended to expand AML/CFT regulations to the crypto ecosystem.[251] The DAAML Act will be reintroduced during the 2023 Congressional session. The DAAML

---

[246] 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.

[247] AMERICAN BANKERS ASSOCIATION, Comment Letter, *Re: Request for Comment on Ensuring Responsible Development of Digital Assets (87 FR 57556)* (Nov. 3, 2022), https://www.aba.com/-/media/documents/comment-letter/cldigitalassets20221103.pdf?rev=fe3a054092fa476490f5bba18bf4bb56; BANK POLICY INSTITUTE, Comment Letter, *Re: Ensuring Responsible Development of Digital Assets; Request for Comment (87 Fed. Reg. 57556 (September 20, 2022))* (Nov. 3, 2022).

[248] *See* U.S. DEP'T OF TREASURY, *supra* note 189, at 10.

[249] *Id.* at 26.

[250] It is unclear whether FinCEN regards NFTs to be "value that substitutes for currency." If NFTs are considered substitutes for currency, then FinCEN could consider NFTs to already be subject to the BSA and FinCEN regulations. Since many NFTs are more like digital representations of ownership in unique, physical assets than value that substitutes for currency, it would appear that many NFTs, including those representing ownership interests in property, should not be subject to FinCEN's oversight; however, business activities related to the transfer, sale, and custody of NFTs likely will implicate FinCEN regulations.

[251] The Digital Asset Anti-Money Laundering Act of 2022, 117th Cong., 2nd Sess. (2022), https://www.warren.senate.gov/imo/media/doc/DAAML%20Act%20of%202022.pdf.

Act would direct FinCEN to designate digital asset wallet providers, miners, validators, and other network participants that may validate, secure, or facilitate digital asset transactions as MSBs and thereby to subject them to responsibilities under the Bank Secrecy Act, including KYC requirements.[252] The DAAML Act would strengthen the enforcement of BSA compliance "by directing the Treasury Department to establish an AML/CFT compliance examination and review process for MSBs and directing the CFTC to establish AML/CFT compliance examination and review processes for the entities it regulates."[253] The DAAML Act also would "extend BSA rules regarding reporting of foreign bank accounts to include digital assets by requiring United States persons engaged in a transaction with a value greater than $10,000 in digital assets through one or more offshore accounts to file a Report of Foreign Bank and Financial Accounts (FBAR) with the Internal Revenue Service."[254]

The DAAML Act would require FinCEN "to finalize and implement its December 2020 proposed rule, which would require banks and MSBs to verify customer and counterparty identities, keep records, and file reports in relation to certain digital asset transactions involving unhosted wallets or wallets hosted in non-BSA compliant jurisdictions."[255] Additionally, the DAAML Act would "prohibit financial institutions from using or transacting with digital asset mixers and other anonymity-enhancing technologies and from handling, using, or transacting with digital assets that have been anonymized using these technologies."[256] Finally, the DAAML Act would require digital asset ATM owners, operators, and administrators to provide the current physical addresses of their kiosks and verify customers' identities.[257]

[252] Senator Elizabeth Warren & Senator Roger Marshall, *The Digital Asset Anti-Money Laundering Act of 2022* (Dec. 13, 2022), https://www.warren.senate.gov/imo/media/doc/Crypto%20National%20Security%20One-Pager%20draft_12.13.22.pdf.
[253] *Id.*
[254] *Id.*
[255] *Id.*; for FinCEN's December 2020 proposed rule, *see* FINCEN, U.S. DEP'T OF TREASURY, Proposed Rule, 87 FR 83840 (2020), https://www.federalregister.gov/documents/2020/12/23/2020-28437/requirements-for-certain-transactions-involving-convertible-virtual-currency-or-digital-assets.
[256] *Id.*
[257] *Id.*

Office of Foreign Assets Control

Introduction

The U.S. Department of the Treasury's Office of Foreign Assets Control ("OFAC") administers and enforces a variety of economic sanctions against countries and regimes, as well as persons (individuals and entities) or groups, such as terrorists, drug kingpins, and those involved in malicious cyber-enabled activities, corruption, and human rights abuses.[258] In recent years, OFAC has increasingly targeted persons engaging in illicit activities through the use of virtual or digital currencies and brought enforcement actions against companies in the virtual currency industry who failed to comply with OFAC sanctions.

OFAC sanctions can be comprehensive or targeted, using the blocking of property or property interests and trade or investment restrictions to accomplish U.S. foreign policy and national security goals. U.S. economic sanctions generally prohibit U.S. persons from engaging in transactions with sanctioned countries, regimes, or persons and entities owned 50 percent or greater by one or more sanctioned persons. In addition, most OFAC sanctions programs prohibit actions taken to circumvent applicable economic sanctions, cause violations of economic sanctions, or to facilitate activities by another person or entity that would violate economic sanctions if undertaken directly. Violations of economic sanctions are subject to criminal and civil penalties, depending on the nature and scope of the violations.

Background on OFAC Actions and Guidance Related to Virtual Currency

Sanctions Designations

Over the past several years, as the use of virtual currencies has increased in the global economy, OFAC has deployed its powerful sanctions authorities against malicious actors in the virtual currency industry or for using virtual currency, such as cryptocurrency, for illicit activity through sanctions designations and blocking of property or property interests.

OFAC has repeatedly sanctioned malicious cyber actors involved in illicit cyber activity and other crimes, including ransomware schemes and money laundering. For example, in 2018, OFAC imposed sanctions against digital currency exchangers who enabled ransomware payments on behalf of Iranian cyber actors involved in the SamSam ransomware scheme.[259] This action marked the first time that OFAC publicly attributed digital currency wallet addresses to sanctioned persons by listing the wallet addresses on OFAC's Specially Designated Nationals and Blocked Persons ("SDN") List in an effort to identify illicit actors operating in the virtual currency space.

Since 2018, OFAC has included more than 150 digital currency wallet addresses on the SDN List.[260] Significantly, OFAC views virtual currency to be property or property interests that falls within the scope of its jurisdiction. By making such identifying information publicly available, OFAC expects U.S. persons and persons otherwise subject to OFAC jurisdiction to screen virtual currency wallet addresses to ensure such identifying information is

[258] OFAC's enforcement authority is limited to civil penalties or remedies. The U.S. Department of Justice ("DOJ") handles criminal violations of sanctions. The DOJ also addresses enforcement through other investigations into conduct that may facilitate sanctions violations, such as money laundering.

[259] U.S. DEP'T OF TREASURY, *Treasury Designates Iran-Based Financial Facilitators of Malicious Cyber Activity and for the First Time Identifies Associated Digital Currency Addresses* (Nov. 28, 2018), https://home.treasury.gov/news/press-releases/sm556.

[260] U.S. DEP'T OF TREASURY, ACTION PLAN TO ADDRESS ILLICIT FINANCING RISKS OF DIGITAL ASSETS, 8 (Sep. 2022), https://home.treasury.gov/system/files/136/Digital-Asset-Action-Plan.pdf, p. 8.

not connected to sanctioned persons. Persons who identify digital currency wallets or other digital currency identifiers believed to be owned by, or otherwise associated with, an SDN and hold such property or property interests are expected to "block" the relevant virtual currency and file a blocking report with OFAC.[261]

Compliance Guidance and Civil Enforcement Actions

In addition to taking sanctions designation actions against cyber actors engaged in illicit activity, OFAC has levied civil monetary penalties against companies in the virtual currency industry for OFAC sanctions compliance failures. The compliance failures were largely the result of sanctions screening deficiencies. Through guidance, including enforcement actions and its "Sanctions Compliance Guidance for the Virtual Currency Industry" ("Virtual Currency Guidance"), OFAC has made clear that "OFAC sanctions compliance obligations apply equally to transactions involving virtual currencies and those involving traditional fiat currencies," and noted the increased risks from transactions in virtual currencies because of the growing prevalence of the use of virtual currencies as a payment method.[262]

OFAC expects U.S. persons and persons otherwise subject to OFAC jurisdiction who operate in the virtual currency industry, including technology companies, exchangers, administrators, miners, wallet providers, and users, to comply with OFAC sanctions—just like persons operating in any other industry.[263] Moreover, OFAC views persons operating in the virtual currency industry as playing increasingly critical roles in the efficacy of OFAC sanctions.[264] Compliance with OFAC sanctions includes not engaging, directly or indirectly, in prohibited transactions, such as dealing in blocked property, engaging in prohibited trade or investment-related transactions, or engaging in transactions that circumvent, or cause a violation of, OFAC sanctions.

OFAC took its first enforcement actions against virtual currency service providers in late 2020 and early 2021, respectively. In December 2020, OFAC announced a $98,830 settlement with BitGo, Inc. ("BitGo"), a technology company that implements security and scalability platforms for digital assets and offers non-custodial secure digital wallet management services, including "hot wallets."[265] BitGo allegedly processed transactions totaling approximately $9,128 for persons located in U.S. sanctioned jurisdictions.[266] As demonstrated in the BitGo settlement and subsequent settlements, OFAC views persons providing digital currency services to be financial service providers.[267]

About two months later, in February 2021, OFAC settled with BitPay, Inc. ("BitPay"), a digital currency payment service provider that offers a payment processing solution for merchants to accept digital currency as payment for goods and services.[268] BitPay ultimately agreed to pay $507,375 to settle its potential civil liability for allowing persons in sanctioned jurisdictions to engage in approximately $129,000 worth of digital currency transactions with BitPay's merchant customers on BitPay's platform.[269]

In both the BitGo and BitPay settlements, OFAC noted that the companies had access to location information, such as IP address data, associated with its users or counterparties (including customers' customers) indicating that the companies were engaging in prohibited transactions. According to OFAC, BitGo and BitPay failed to leverage available location information for sanctions compliance purposes, which resulted in apparent violations of

---

[261] *See* OFAC Frequently Asked Questions ("FAQs") 562; *see also* OFAC FAQ 646 (explaining how to block digital currency).
[262] *See* OFFICE OF FOREIGN ASSETS CONTROLS, SANCTIONS COMPLIANCE GUIDANCE FOR THE VIRTUAL CURRENCY INDUSTRY, 1 (Oct. 2021), https://home.treasury.gov/system/files/126/virtual_currency_guidance_brochure.pdf; *see also* OFAC FAQ 560 (reiterating that OFAC compliance obligations are the same, regardless of whether a transaction is denominated in digital or traditional fiat currency).
[263] *See* OFFICE OF FOREIGN ASSETS CONTROLS, SANCTIONS COMPLIANCE GUIDANCE FOR THE VIRTUAL CURRENCY INDUSTRY, 1 (Oct. 2021).
[264] *See id*.
[265] U.S. DEP'T OF TREASURY, *OFAC Enters Into $98,830 Settlement with BitGo, Inc. for Apparent Violations of Multiple Sanctions Programs Related to Digital Currency Transaction* (Dec. 30, 2020), https://home.treasury.gov/system/files/126/20201230_bitgo.pdf.
[266] *Id*.
[267] *Id*. at 3.
[268] U.S. DEP'T OF TREASURY, *OFAC Enters Into $507,375 Settlement with BitPay, Inc. for Apparent Violations of Multiple Sanctions Programs Related to Digital Currency Transactions* (Feb. 18, 2021), https://home.treasury.gov/system/files/126/20210218_bp.pdf. p. 1.
[269] *Id*.

OFAC sanctions. Although IP address blocking is an imperfect screening tool, OFAC has clearly conveyed through multiple enforcement actions, including BitGo and BitPay, and other guidance its expectations that companies utilize IP blocking or other geolocation verifying and blocking tools.

Significant OFAC Actions Related to Virtual Currency in 2022

Sanctions Designations

During 2022, OFAC continued to take sanctions designation actions in the virtual currency space, underscoring OFAC's important role in countering malicious actors using virtual currency for illicit activity. For example, on April 5, 2022, OFAC sanctioned Garantex, a virtual currency exchange originally registered in Estonia with the majority of its operations carried out in Russia, for its involvement in transactions with illicit actors and darknet markets, including the world's largest and most prominent darknet market, Hydra Market in Russia.[270] The action was taken by OFAC in collaboration with the U.S. Department of Justice, Federal Bureau of Investigations, Drug Enforcement Administration, Internal Revenue Service Criminal Investigation, and Homeland Security Investigations, as well as through cooperation with international partners.[271]

On April 20, 2022, in a major action against facilitators of Russia's attempt to evade U.S. sanctions against Russia for its aggression towards Ukraine, OFAC sanctioned virtual currency mining company Bitriver AG and ten of its Russian-based subsidiaries for their involvement in Russia's virtual currency mining industry that Russia used for sanctions evasion.[272] When announcing the designations, Treasury stated that the United States "is committed to ensuring that no asset, no matter how complex, becomes a mechanism for the Putin regime to offset the impact of sanctions."[273]

Another notable sanctions action includes OFAC's August 8, 2022 designation of the virtual currency mixer Tornado Cash.[274] OFAC sanctioned Tornado Cash for its involvement in laundering more than $7 billion worth of virtual currency, including over $455 million stolen by the Lazarus Group, a North Korean state-sponsored hacking group that was sanctioned by OFAC in 2019.[275] Tornado Cash also was used to launder more than $96 million of funds derived from the June 24, 2022 Harmony Bridge Heist and at least $7.8 million from the August 2, 2022 Nomad Heist.[276]

OFAC's sanctions designations in 2022 demonstrate Treasury's ongoing commitment and work to expose the virtual currency ecosystem components that cybercriminals use to obfuscate proceeds from illicit cyber activity and other crimes, like fraud and money laundering. As Treasury has noted, while most virtual currency activity is legitimate, it can be used for illicit activity through, for example, mixers, P2P exchangers, darknet markets, and exchanges.[277] Treasury will continue to use its authorities—including sanctions authorities implemented by OFAC—against malicious cyber actors in coordination with other U.S. Government agencies and international partners "to expose, disrupt, and hold accountable perpetrators and persons that enable criminals to profit from cybercrime and other illicit activity."[278]

Civil Enforcement Actions

In 2022, OFAC also continued to impose civil penalties against companies operating in the virtual currency industry for sanctions compliance failures. On October 11, 2022, OFAC announced that Bittrex, an online virtual currency exchange and hosted wallet service provider, agreed to pay $24,280,829.20 to settle its civil liability for apparent violations of multiple sanctions programs.[279] According to OFAC, as a

---

[270] U.S. DEP'T OF TREASURY, *Treasury Sanctions Russia-Based Hydra, World's Largest Darknet Market, and Ransomware-Enabling Virtual Currency Exchange Garantex* (Apr. 5, 2022), https://home.treasury.gov/news/press-releases/jy0701.
[271] *See id.*
[272] *See* U.S. DEP'T OF TREASURY, *U.S. Treasury Designates Facilitators of Russian Sanctions Evasion* (Apr. 20, 2022), https://home.treasury.gov/news/press-releases/jy0731.
[273] *Id.*
[274] U.S. DEP'T OF TREASURY, *U.S. Treasury Sanctions Notorious Virtual Currency Mixer Tornado* (Aug. 8, 2022), https://home.treasury.gov/news/press-releases/jy0916.
[275] *Id.*
[276] *Id.*
[277] *Id.*
[278] *Id.*
[279] U.S. DEP'T OF TREASURY, *OFAC Settles with Bittrex, Inc. for $24,280,829.20 Related to Apparent Violations of Multiple Sanctions Programs* (Oct. 11, 2022), https://home.treasury.gov/system/files/126/20221011_bittrex.pdf, p. 1.

result of deficiencies in Bittrex's sanctions compliance program, Bittrex failed to prevent persons located in U.S. sanctioned jurisdictions from engaging in virtual currency transactions.[280]

OFAC stated that Bittrex failed to implement any sanctions compliance program or verifying of customer identify until over a year and a half after first offering virtual currency services, and that, only after receiving an administrative subpoena from OFAC, did Bittrex implement internal controls to screen customers or transactions, which was over three years after first offering virtual currency services.[281] Similar to BitGo and BitPay, OFAC also stated that Bittrex had reason to know that users were in sanctioned jurisdictions based on location information available to Bittrex, including IP address data.[282] The Bittrex settlement demonstrates OFAC's expectations that new companies, including those in the virtual currency industry, incorporate sanctions compliance into business functions at the outset of business and screen for location information.[283]

Importantly, as noted in Section VII, OFAC's settlement with Bittrex was part of a global resolution with Treasury's FinCEN, demonstrating OFAC and FinCEN's collaboration on matters that involve sanctions and AML issues. We expect to see additional enforcement collaboration between OFAC and FinCEN in the future.

More recently, on November 28, 2022, OFAC settled with Payward, Inc. d/b/a/ Kraken ("Kraken"), a virtual currency exchange, for $362,158.70 to settle Kraken's potential civil liability for apparent violations of comprehensive sanctions imposed on Iran by OFAC.[284] As part of the settlement with OFAC, Kraken also agreed to invest $100,000 in certain internal sanctions compliance controls.[285]

In the settlement announcement, OFAC stated that Kraken maintained an anti-money laundering and sanctions compliance program, which included screening customers at onboarding and on a daily basis thereafter, as well as reviewing IP address information generated at the time of onboarding to prevent users in sanctioned jurisdictions from opening accounts.[286] Despite these controls, Kraken processed transactions totaling approximately $1,680,577.10 on behalf of persons who appeared to have been located in Iran at the time of the transactions because Kraken did not implement IP address blocking on *transactional* activity across its platform.[287] As noted by OFAC, according to IP address data, certain account holders who established accounts outside of Iran appear to have accessed their accounts and transacted on Kraken's platform from Iran.[288]

In the Kraken settlement, OFAC yet again underscored the importance of using geolocation verifying and blocking tools, such as IP address blocking, to prevent users located in sanctioned jurisdictions from engaging in virtual currency transactions prohibited by OFAC sanctions. Additionally, the Kraken settlement highlights how technology companies, including those offering virtual currency-related services, should be screening accounts at the time of opening and account transactions throughout the duration of the account to reduce sanctions risks.

Outlook for 2023

OFAC's continued efforts to designate malicious actors in the virtual currency space and bring enforcement actions against persons operating in the virtual currency industry for compliance failures signifies OFAC's important role in the United States whole-of-government efforts with respect to virtual currency. OFAC is likely to impose more designations and enforcement actions in the virtual currency space in 2023.

On March 31, 2023, OFAC issued its first enforcement action for 2023 related to digital currency services when Uphold HQ Inc. ("Uphold"), a money services business, agreed to pay OFAC $72,230.32 to settle Uphold's potential civil liability for apparent violations of multiple sanctions programs

---

[280] *Id.*
[281] *See id.* at 1-2.
[282] *See id.* at 1.
[283] *See id.* at 4.
[284] U.S. DEP'T OF TREASURY, *OFAC Settles with Virtual Currency Exchange Kraken for $362,158.70 Related to Apparent Violations of the Iranian Transactions and Sanctions Regulations* (Nov. 28, 2022), https://home.treasury.gov/system/files/126/20221128_kraken.pdf, p. 1.
[285] *See id.*
[286] *Id.*
[287] *Id.*
[288] *See id.*

administered by OFAC.[289] Uphold is a global multi-asset digital trading platform where customers can move, convert, and hold traditional and virtual currency or commodities to enable foreign exchange and cross-border remittances.[290]

According to OFAC's settlement announcement, Uphold, or certain of its non-U.S. affiliates, maintained accounts for customers who provided information during the account onboarding process indicating their location was in sanctioned jurisdictions.[291] In addition, Uphold processed transactions on behalf of two customers who self-identified in the course of enhanced customer diligence as employees of the Government of Venezuela.[292]

The Uphold settlement again demonstrates OFAC's view that those that provide services related to virtual currencies are obliged to comply with OFAC sanctions and should maintain risk-based compliance programs with robust controls to identify sanctions risk, including for purposes of screening identification and location information provided by customers.[293]

Establishing an effective risk-based OFAC sanctions compliance program is essential for those operating in the virtual currency industry. As emphasized by OFAC through numerous enforcement actions, including those discussed above, and OFAC's Virtual Currency Guidance and 2019 "A Framework for OFAC Compliance Commitments,"[294] OFAC expects sanctions compliance programs to include the following five key elements: (1) management commitment; (2) risk assessments; (3) internal controls; (4) testing and auditing; and (5) training. Companies operating in the virtual currency industry should assess their current compliance programs to ensure the sanctions compliance programs include the aforementioned elements and are commensurate with the company's size, operations, and risk profile.

Importantly, companies operating in the virtual currency industry should ensure that their sanctions compliance programs are utilizing available technology to verify the identity and location of users and counterparties, including blockchain analytics tools to assist with sanctions screening and monitoring. OFAC expects companies to leverage technological solutions for sanctions compliance to help mitigate sanctions risks.[295] Companies also should take stock of what information is being collected in the ordinary course of business on users and counterparties and assess whether that information is relevant to sanctions compliance (*i.e.*, provides identity and location information) and is or should be screened for sanctions compliance purposes. If companies are not already utilizing IP address blocking or other geolocation verifying and blocking tools, companies should seriously consider implementing those or similar tools based on OFAC's clear expectation that such tools be utilized for sanctions compliance purposes.

---

[289] U.S. DEP'T OF TREASURY, *OFAC Settles with Uphold HQ Inc. for $72,230.32 Related to Apparent Violations of Multiple Sanctions Programs* (Mar. 31, 2023), https://ofac.treasury.gov/media/931556/download?inline, p. 1.

[290] *Id.*

[291] *Id.*

[292] *Id.* at 2. OFAC previously blocked the Government of Venezuela and any political subdivision, agency, or instrumentality thereof, including any person who has acted or purported to act directly or indirectly for or on behalf of the Venezuelan Government.

[293] *Id.* at 3.

[294] U.S. DEP'T OF TREASURY, A FRAMEWORK FOR OFAC COMPLIANCE COMMITMENTS (May 2019), https://home.treasury.gov/system/files/126/framework_ofac_cc.pdf.

[295] *See* VIRTUAL CURRENCY GUIDANCE, pp. 14-15; *see also* SANCTIONS COMPLIANCE GUIDANCE FOR INSTANT PAYMENT SYSTEMS, OFFICE OF FOREIGN ASSETS CONTROL, 2-3. (Sept. 2022), https://home.treasury.gov/system/files/126/instant_payment_systems_compliance_guidance_brochure.pdf.

Committee on Foreign Investment in the United States

Introduction

The Committee on Foreign Investment in the United States ("CFIUS") is an interagency committee authorized to review transactions involving foreign investment in the United States and certain real estate transactions by non-U.S. persons to determine the effect of such transactions on U.S. national security. For purposes of CFIUS, a U.S. entity controlled or that becomes controlled by a non-U.S. person may trigger CFIUS's jurisdiction.

Filings with CFIUS are largely voluntary. However, in certain circumstances, filings with CFIUS are mandatory, and CFIUS is authorized to penalize both parties up to the value of the transaction for a failure to submit a mandatory filing. Importantly, regardless of whether a filing is voluntary or mandatory, CFIUS also has the authority to initiate a review post-closing and impose restrictions or, in rare cases, force the non-U.S. investor to divest its stake.

CFIUS's involvement in the virtual currency industry and others in the financial technology sector arises when U.S. companies involved with cryptocurrency seek investment from non-U.S. investors. Therefore, it is important for participants in the virtual currency industry to understand CFIUS's jurisdiction, how non-U.S. investments in their business could trigger CFIUS's jurisdiction, and how CFIUS's assessments of U.S. national security risks may apply to their respective businesses.

Background on CFIUS and Its Impact on the Virtual Currency Industry

CFIUS Jurisdiction and Cryptocurrency Businesses

CFIUS has jurisdiction over "covered control transactions" and "covered investments."[296] Filings for both types of jurisdictions can either be voluntary or mandatory. An investment is a covered control transaction when a non-U.S. investor directly or indirectly acquires "control" over a U.S. business.[297] CFIUS construes "control" broadly as the power, whether exercised or not, to determine, direct, take, reach, or cause decisions regarding important matters affecting the U.S. business (*i.e.*, it is not a fifty percent or greater ownership rule).[298] CFIUS can find control in as low as ten percent investment, and even lower than ten percent if the non-U.S. investor acquires important rights, particularly where the transaction presents U.S. national security risks (*e.g.*, due to the nature of the U.S. business or the identity of the non-U.S. investor). When examining a non-U.S. investor's interest in a U.S. business, CFIUS can aggregate the interests of different non-U.S. investors that are ultimately owned by the same entity or have an agreement to act in concert regarding their respective interests in the U.S. business. Notably, certain purely passive investments are carved out of CFIUS's "covered control" jurisdiction when a non-U.S. investor acquires ten percent or less of the outstanding voting interest in a U.S. business (regardless of U.S. dollar value) solely for the purpose of passive investment.

---

[296] CFIUS also has jurisdiction over "covered real estate transactions," which are transactions in which: (1) there is no existing U.S. business (*e.g.*, the non-U.S. investor is purchasing vacant land); (2) the land is within certain proximities of certain sensitive U.S. Government facilities; and (3) the non-U.S. investor will acquire three of the following property rights that give the investor the ability:
To physically access the real estate;
To exclude others from physically accessing the real estate;
To improve or develop the real estate; or
To attach fixed or immovable structures or objects to the real estate. 31 C.F.R. § 802.212.

[297] 31 C.F.R. § 800.210.

[298] 31 C.F.R. § 800.208.

As with other U.S. businesses, cryptocurrency businesses should assess whether investments by non-U.S. persons through which the non-U.S. person acquires a greater than ten percent interest or rights that could give the non-U.S. person control over the business trigger CFIUS' jurisdiction over covered control transactions.

A "covered investment" is a transaction in which a non-U.S. person makes a direct or indirect non-controlling investment in a U.S. business involved in critical technology, critical infrastructure, or collecting or maintaining the sensitive personal data of U.S. citizens.[299] Together, these businesses are known as "TID U.S. businesses" (Technology, Infrastructure, Data).

In some circumstances, parties may be required to make a mandatory CFIUS filing for a covered investment or a covered control transaction. Specifically, CFIUS has mandatory filing jurisdiction over covered investments and covered control transactions by non-U.S. persons in TID U.S. businesses that design, fabricate, develop, test, produce, or manufacture one or more "critical technologies" if: (1) a U.S. regulatory authorization (*e.g.,* an export license) would be required to export, reexport, transfer, or retransfer the critical technology to the non-U.S. investor, regardless of whether such critical technology is, in fact, exported to the non-U.S investor; or (2) a non-U.S. person or group of non-U.S. persons holds a "substantial interest" in a TID U.S. business (*i.e.*, twenty-five percent or greater direct or indirect voting interest, and where a foreign government holds a forty-nine percent or greater interest in the non-U.S. investor).

In the case of non-controlling covered investments, the non-U.S. investor also must acquire: (1) access to the TID U.S. business's material nonpublic technical information; (2) membership, observer, or nomination rights on the TID U.S. business's board of directors; or (3) any involvement, other than by voting shares, in the TID U.S. business's substantive decision-making. There are several ways in which cryptocurrency businesses could qualify as TID U.S. businesses and trigger CFIUS's jurisdiction over covered investments.

- First, many of the products, software, and technology used by cryptocurrency businesses may be "critical technologies" as defined by CFIUS regulations because they are controlled under U.S. export controls due to advanced technological capabilities or encryption functionalities.[300] Notably, even if a business's distributed ledger or blockchain technology that enables the existence of its cryptocurrency does not fall within the regulatory CFIUS definition of "critical technology," CFIUS may still seek to assess transactions involving non-U.S. investment in cryptocurrency businesses because the U.S. Government views distributed ledger technology more generally as a critical and emerging technology.
- Second, "sensitive person data" includes categories that may be relevant to cryptocurrency businesses, such as the set of data in a consumer report, financial data that could be used to analyze or determine an individual's financial distress or hardship, or non-public electronic communications, including email, messaging, or chat communications. In addition, the U.S. Government has increasingly focused on the protection of U.S. citizens' data and, even if a cryptocurrency business's data does not fall within the CFIUS definition of "sensitive personal data," CFIUS may still seek to scrutinize transactions involving non-U.S. investors if the cryptocurrency business holds U.S. citizens' personally identifiable information ("PII").

CFIUS National Security Risk Assessments and Cryptocurrencies

CFIUS broadly defines "national security" based on a number of factors contained in the Defense Production Act of 1950, as amended, including: the control of domestic industries and commercial activity by non-U.S. citizens; whether the transaction is non-U.S. Government-controlled; whether the non-U.S. buyer's country is a U.S. ally, supports U.S. counter-terrorism efforts, and/or adheres to arms control and nonproliferation treaties; and all other facts that it "may determine to be appropriate, generally or in

[299] 31 C.F.R. § 800.211.

[300] *See* 31 C.F.R. § 800.215.

connection with a specific review or investigation."[301] This final miscellaneous factor allows CFIUS to weigh additional national security risks, such as the concerns expressed throughout the U.S. Government regarding the use of cryptocurrency for illicit cyber activities and other crimes, efforts by the U.S. Government to protect U.S. leadership in crypto technology, and U.S. Government concerns about protecting U.S. citizens' data.

As mentioned, although a cryptocurrency business's distributed ledger technology may not be "critical technology" as defined by CFIUS regulations, the U.S. Government more broadly considers "Distributed Ledger Technologies" a critical and emerging financial technology important to U.S. national security, which could result in CFIUS seeking to review a transaction.[302] In addition, the U.S. Government is increasingly focused on efforts to protect U.S. citizens' personal data, and those efforts are likely to be carried over to CFIUS's assessments of national security risk as well.[303]

Notably, when assessing the national security risk factors, CFIUS considers: (1) the threat posed by the buyer; (2) the vulnerabilities of the U.S. business; and (3) the consequences if the buyer exploits the U.S. business. CFIUS considers each of the foregoing factors using a worst-case-scenario approach, meaning CFIUS may view some investments by even seemingly benevolent non-U.S. investors as a risk to U.S. national security.

Significant CFIUS Activity Related to Cryptocurrency in 2022

CFIUS filings and the review process are confidential and not publicly available unless parties to a transaction make the information public. As a result, there is limited publicly available information about CFIUS reviews, including in relation to cryptocurrency. However, there were public reports in 2022 indicating that concerns about CFIUS were an important factor in a bid by Binance, a virtual currency exchange whose founder and CEO was born in China but grew up in Canada, to acquire Voyager Digital's assets following Voyager Digital's bankruptcy.[304] During bankruptcy proceedings where Voyager Digital sought the court's approval to sell Voyager Digital's assets to Binance, CFIUS submitted a notice to the court that the sale could be subject to CFIUS' review and Voyager Digital's attorney acknowledged that the company has been engaged with CFIUS.[305]

In 2022, the Biden Administration also directed CFIUS to consider national security risks in its assessments that could impact cryptocurrency businesses. Specifically, President Biden issued Executive Order 14083, titled "Ensuring Robust Consideration of Evolving National Security Risks by the Committee on Foreign Investment in the United States," which directs CFIUS to consider several risk factors that could relate to cryptocurrency businesses, such as the effects of transactions on U.S. technological leadership, U.S. cybersecurity, and U.S. sensitive data security.[306]

Outlook for 2023

CFIUS's importance for companies seeking non-U.S. investment has grown substantially. In 2009, CFIUS reviewed 65 transactions.[307] In 2021, CFIUS reviewed more than 300 transactions.[308] In addition to its specific task of reviewing transactions for national security concerns, U.S. Government agencies have emphasized CFIUS's importance as a tool to provide

---

[301] 50 U.S.C. § 4565.

[302] *See* NAT'L SCI. AND TECH. COUNCIL, *CRITICAL AND EMERGING TECHNOLOGIES LIST UPDATE* (Feb. 2, 2022), https://www.whitehouse.gov/wp-content/uploads/2022/02/02-2022-Critical-and-Emerging-Technologies-List-Update.pdf.

[303] *See, e.g.*, Exec. Order No. 14,034, *Protecting Americans' Sensitive Data From Foreign Adversaries* (June 9, 2021), https://www.govinfo.gov/content/pkg/FR-2021-06-11/pdf/2021-12506.pdf.

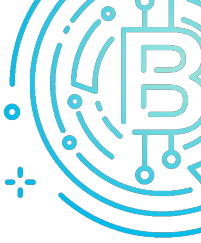
[304] *See* Ian Allison, *Binance's Attempt to Buy Voyager Digital's Assets Complicated by National Security Concern: Sources*, COINDESK (Sep. 16, 2022), https://www.coindesk.com/business/2022/09/16/binances-attempt-to-buy-voyager-digitals-assets-complicated-by-national-security-concern-source/.

[305] *See Voyager Digital Holdings, Inc.*, No. 22-10943 (MEW), Dkt. No. 797 (Bankr. S.D.N.Y. 2022); *see also* Luke Huigsloot, *Voyager and Binance US deal Given Initial Nod Amid National Security Probe*, COINTELEGRAPH (Jan. 11, 2023), https://cointelegraph.com/news/initial-approval-given-for-voyager-and-binance-us-deal-amid-national-security-probe.

[306] *See* Exec. Order No. 14,083, *Ensuring Robust Consideration of Evolving National Security Risks by the Committee on Foreign Investment in the United States* (Sep. 15, 2022), https://www.govinfo.gov/content/pkg/FR-2022-09-20/pdf/2022-20450.pdf.

[307] *See* COMM. ON FOREIGN INV. IN THE U.S., *Annual Report to Congress* (Nov. 2010), https://home.treasury.gov/system/files/206/CFIUS-Annual-Report-to-Congress-for-CY09.pdf.

[308] *See* COMM. ON FOREIGN INV. IN THE U.S., *Annual Report to Congress* (Aug. 2022), https://home.treasury.gov/policy-issues/international/the-committee-on-foreign-investment-in-the-united-states-cfius/cfius-reports-and-tables.



the U.S. Government with information about current trends and developments in the market, especially as they relate to technologies the U.S. Government views as important to U.S. national security. Therefore, companies involved in the virtual currency industry that seek non-U.S. investment should be familiar with CFIUS, what triggers its jurisdiction, whether the company is involved with "critical technology" or "sensitive personal data" that could trigger a mandatory filing with CFIUS, and the potential national security concerns that non-U.S. investors could present, even if a mandatory CFIUS filing is not required.

State Regulatory Actions

At the state level, cryptocurrency regulations and enforcement actions are on the rise. As a sign of the extent of state-level interest, at least 37 states and Puerto Rico considered cryptocurrency-related legislation during the 2022 legislative session.

From virtual currency tax exemptions in Alabama,[309] to licensing requirements in Hawai'i[310] and Kentucky,[311] to money transmission regulations in Mississippi,[312] and digital asset disclosure requirements in Pennsylvania,[313] states across the country have shown significant interest, and varying levels of progress in expanding existing regulatory regimes to cover digital assets.[314]

In the wake of the "crypto winter" and associated perceived shortcomings in consumer protections and oversight, states are already increasing their enforcement efforts in 2023.

State Enforcement Actions and Guidance

On April 8, 2022, the Attorney General Alliance ("AGA")[315] released a collaborative White Paper encouraging state attorneys general to "engage with th[e] new – and ever growing" digital asset industry.[316] The White Paper outlined how state regulators can assert their authority to better protect consumers, and provided a foundational understanding of how blockchain and wallet technologies operate, summarized the basics of cryptocurrency mining, and outlined different types of coins, tokens, and NFTs.[317] The AGA also emphasized the role that state Attorneys General have in filling gaps in federal regulations by (1) collaborating in multi-jurisdictional investigations, (2) sharing available resources and expertise, (3) investigating individual cases, and (4) working with federal law enforcement agencies where appropriate.[318]

Multi-State Actions

States are already enacting the approach advocated by the AGA. On September 26, 2022, for example, eight states (California, Kentucky, Maryland, New York, Oklahoma, South Carolina, Washington, and Vermont) filed coordinated legal actions against Nexo for failing to register with state regulators.[319] The states collectively alleged Nexo, a cryptocurrency lending platform, had failed to register with the states as securities and commodities brokers or dealers and had lied to investors about Nexo's registration

[309] *See* H.B. 127, 2022 Leg., (Al. 2022), http://alisondb.legislature.state.al.us/ALISON/SearchableInstruments/2022RS/PrintFiles/HB127-int.pdf.
[310] *See* H.B. 2108, 2022 Leg., (Haw. 2022), https://www.capitol.hawaii.gov/sessions/session2022/bills/HB2108_SD2_.htm.
[311] *See* H.B. 724, 2022 Leg., (Ky. 2022), https://apps.legislature.ky.gov/record/22rs/hb724.html.
[312] *See* H.B. 1152, 2022 Leg. (Miss. 2022), http://billstatus.ls.state.ms.us/documents/2022/pdf/HB/1100-1199/HB1152IN.pdf.
[313] *See* S.B. 399, 2021 Gen. Assemb., (Pa. 2021), https://www.legis.state.pa.us/CFDOCS/Legis/PN/Public/btCheck.cfm?txtType=PDF&sessYr=2021&sessInd=0&billBody=S&billTyp=B&billNbr=0399&pn=0347.
[314] For a collection of state legislative activity regarding cryptocurrency, *see* Cryptocurrency 2022 Legislation, NATIONAL CONFERENCE OF STATE LEGISLATURES (May 7, 2023), https://www.ncsl.org/financial-services/cryptocurrency-2022-legislation.
[315] The AGA is an alliance of state Attorneys General, federal, state, and foreign officials, and public and private sector partners that focus on addressing complex issues in law and policy. The AGA's network reaches 46 states and territories, and is built on a foundation of fostering collaboration between state Attorneys General offices. *See* Our Mission, ATTORNEY GENERAL ALLIANCE (May 7, 2023), https://www.agalliance.org/about/.
[316] Attorney General Alliance - Digital Assets White Paper, ATTORNEY GENERAL ALLIANCE (Apr. 8, 2022), https://files.constantcontact.com/48922045201/588b8eba-571d-4075-a708-69c6dda04cc5.pdf.
[317] *Id.* at 2–7.
[318] *Id.* at 9-11.
[319] *See* NEW YORK OFFICE OF THE ATTORNEY GENERAL, *Attorney General James Sues Cryptocurrency Platform for Operating Illegally and Defrauding Investors* (Sept. 26, 2022), https://ag.ny.gov/press-release/2022/attorney-general-james-sues-cryptocurrency-platform-operating-illegally-and.

status.[320] The states coordinated their investigations through a working group of multi-state securities regulators. On January 19, 2023, the multistate coalition secured a settlement of $22.5 million from Nexo Inc.[321] [322] As part of the settlement, Nexo also agreed to be barred from the New York securities industry for five years.[323]

In another instance, Texas, Kentucky, and Alabama coordinated cease and desist orders against Slotie NFT, a metaverse casino.[324] On October 20, 2022, the three states accused Slotie NFT of illegally and fraudulently selling nonfungible tokens to raise capital for online casinos.[325] Slotie had allegedly misled investors through issuing its own ERC-721 token without informing investors of its anticipated use of capital, the identity of partnering casinos, and its assets and liabilities.[326] In total, the states accused Slotie of issuing over 10,000 Slotie NFTs that were similar to stock and other equities.[327]

Additional State Enforcement Actions

Throughout 2022, a number of states acted individually in pursuing enforcement actions for the cryptocurrency industry as well.

- **New Jersey** filed a cease and desist order against Voyager Digital in March 2022.[328] The Attorney General of New Jersey and the New Jersey Bureau of Securities alleged that Voyager had sold unregistered securities in the form of interest-earning cryptocurrency accounts that had raised upwards of $5 billion across the nation.[329] This is the third time New Jersey has acted against a New Jersey based cryptocurrency firm, including BlockFi Lending in July 2021[330] and Celsius Network in September 2021.[331]
- On August 3, 2022, the **New York** Department of Financial Services ("DFS") announced cryptocurrency trading platform Robinhood had agreed to pay a $30 million penalty for failing to allocate sufficient resources to meet its compliance obligations under the Department's virtual currency regulations.[332] The state alleged that Robinhood's transaction monitoring system had inadequate protocols in place to recognize fraudulent or nefarious transactions, its anti-money laundering program was insufficiently staffed, and its cybersecurity protections had significant failures exposing consumer data and transactions to ill-intentioned actors.[333]
- In July 2022, the **California** Department of Financial Protection and Innovation ("DFPI") announced a series of investigations into companies across the country that offer customers interest-bearing crypto asset accounts

---

[320] *See* Complaint, *New York v. Nexo Inc.*, (N.Y. Sup. Ct. 2022), https://ag.ny.gov/sites/default/files/2022.09.26_nexo_complaint_final.pdf.
[321] *See* NEW YORK OFFICE OF THE ATTORNEY GENERAL, *Attorney General James and Multistate Coalition Secure $24 Million from Cryptocurrency Platform Nexo for Operating Illegally* (Jan. 19, 2023), https://ag.ny.gov/press-release/2023/attorney-general-james-and-multistate-coalition-secure-24-million-cryptocurrency.
[322] *See* CALIFORNIA DEPARTMENT OF FINANCIAL PROTECTION & INNOVATION, *California Joins $22.5 Million Multistate Securities Settlement Against Crypto Platform Nexo Capital* (Jan. 26, 2023), https://dfpi.ca.gov/2023/01/26/california-joins-22-5-million-multistate-securities-settlement-against-crypto-platform-nexo-capital/.
[323] *See* Stipulation and Consent, *New York v. Nexo Inc.,* Index No. 452610/2022, (N.Y. Sup. Ct. 2022), https://ag.ny.gov/sites/default/files/ny nexo_stipulation_and_proposed_order_and_judgment.pdf.
[324] *See* TEXAS STATE SECURITIES BOARD, *Three State Securities Regulators File Enforcement Actions to Stop Sales of Fraudulent NFT Investments Tied to the Metaverse* (Oct. 20, 2022), https://www.ssb.texas.gov/news-publications/three-state-securities-regulators-file-enforcement-actions-stop-sales-fraudulent.
[325] *Id.*
[326] *Id.*
[327] *Id.*
[328] *See* NEW JERSEY DIVISION OF CONSUMER AFFAIRS, *New Jersey Bureau of Securities Orders Cryptocurrency Company 'Voyager Digital' to Stop Offering and Selling Interest-Bearing Accounts* (Mar. 29, 2022), https://www.njconsumeraffairs.gov/News/Pages/03292022.aspx.
[329] *Id.*
[330] *See* NEW JERSEY DIVISION OF CONSUMER AFFAIRS, *New Jersey Bureau of Securities Orders Cryptocurrency Company 'BlockFi' to Stop Offering Interest-Bearing Accounts* (July 20, 2021), https://www.njconsumeraffairs.gov/News/Pages/07202021.aspx.
[331] *See* NEW JERSEY DEPARTMENT OF LAW & PUBLIC SAFETY, *New Jersey Bureau of Securities Orders Cryptocurrency Firm Celsius to Halt the Offer and Sale of Unregistered Interest-Bearing Investments* (Sept. 17, 2021), https://www.njoag.gov/new-jersey-bureau-of-securities-orders-cryptocurrency-firm-celsius-to-halt-the-offer-and-sale-of-unregistered-interest-bearing-investments/.
[332] *See* NEW YORK DEPARTMENT OF FINANCIAL SERVICES, *DFS Superintendent Harris Announces $30 Million Penalty On Robinhood Crypto for Significant Anti-Money Laundering, Cybersecurity & Consumer Protection Violations*, https://www.dfs.ny.gov/reports_and_publications/press_releases/pr202208021.
[333] *Id.*

or "crypto-interest accounts."[334] Similar to Voyager Digital in New Jersey, these accounts allowed customers to lend crypto assets to the company in exchange for interest paid in crypto assets.[335] The DFPI focused on risk disclosures and warned that consumers may not have had complete information from these companies prior to making deposits on crypto platform(s) in question.[336] DFPI has not made public the results of some of those investigations, but announced that it entered into a $22.5 million multi-state settlement against Nexo Group (see above)[337] and is seeking the revocation of Celsius Lending's California Financing Law license.[338]

- Another enforcement action from **California** focused on consumer protection in the wake of 2022's crypto winter. On November 11, 2022, DFPI moved to suspend BlockFi's lending license for 30 days following FTX's bankruptcy filing while the Department investigated BlockFi's plan to pause client withdrawals.[339] BlockFi initially announced via Twitter that it could not "operate business as usual" given the "lack of clarity on the status of FTX.com, FTX US and Alameda," and limited account activity on the platform including by pausing withdrawals.[340] This statement caused the DFPI to launch a broader investigation into BlockFi's compliance with California's Financing Law and Consumer Financial Protection Law.[341]

These trends have continued throughout 2023. In New York, for example, DFS announced a $100 million settlement with Coinbase, Inc. ("Coinbase") in January after a DFS investigation found "significant failures" in Coinbase's compliance program.[342] Although Coinbase had been licensed by DFS to conduct a virtual currency business and money transmitting business since 2017, the DFS investigation found that Coinbase's Bank Secrecy Act/Anti-Money Laundering program—including its Know Your Customer/Customer Due Diligence ("KYC/CDD"), Transaction Monitoring System ("TMS"), suspicious activity reporting, and sanctions compliance systems—were "inadequate for a financial services provider of Coinbase's size and complexity."[343] As part of the settlement, Coinbase agreed to pay $50 million in penalties for "significant failures in its compliance program that violated the New York Banking Law and the New York State Department of Financial Services' ("DFS") virtual currency, money transmitter, transaction monitoring, and cybersecurity regulations," as well as invest another $50 million in compliance functions "over the next two years to remediate the issues and to enhance its compliance program pursuant to a plan approved by DFS."[344]

In February and March 2023, New York Attorney General Letitia James sued cryptocurrency platforms CoinEx and KuCoin for "failing to register as a securities and commodities broker-dealer and for

---

[334] *See* CALIFORNIA DEPARTMENT OF FINANCIAL PROTECTION & INNOVATION, *DFPI is actively investigating multiple companies offering "crypto-interest accounts"* (July 12, 2022), https://dfpi.ca.gov/2022/07/12/dfpi-is-actively-investigating-multiple-companies-offering-crypto-interest-accounts/.

[335] *Id.*

[336] *Id.*

[337] *See* CALIFORNIA DEPARTMENT OF FINANCIAL PROTECTION & INNOVATION, *California Joins $22.5 Million Multistate Securities Settlement Against Crypto Platform Nexo Capital* (Jan. 26, 2023), https://dfpi.ca.gov/2023/01/26/california-joins-22-5-million-multistate-securities-settlement-against-crypto-platform-nexo-capital/.

[338] *See* CALIFORNIA DEPARTMENT OF FINANCIAL PROTECTION & INNOVATION, *DFPI initiates revocation of Celsius Lending LLC's CFL Lending License* (Aug. 24, 2022), https://dfpi.ca.gov/2022/08/24/dfpi-initiates-revocation-of-celsius-lending-llcs-cfl-lending-license/#:~:text=DFPI%20initiates%20revocation%20of%20Celsius%20Lending%20LLC's%20CFL%20Lending%20License,-Aug%2024%2C%202022&text=On%20August%2019%2C%202022%2C%20the,resolution%20of%20the%20revocation%20action.

[339] *See* CALIFORNIA DEPARTMENT OF FINANCIAL PROTECTION & INNOVATION, *Crypto Lender BlockFi Agrees to Provide More Than $100,000 in Refunds to Californians* (Mar. 27, 2023), https://dfpi.ca.gov/2023/03/27/crypto-lender-blockfi-agrees-to-provide-more-than-100000-in-refunds-to-californians/.

[340] *See* BlockFi (@BlockFi), TWITTER (Nov. 10, 2022, 5:16 PM), https://twitter.com/BlockFi/status/1590875997351866368?cxt=HHwWgMDT_c3S9pMsAAAA.

[341] *See* CALIFORNIA DEPARTMENT OF FINANCIAL PROTECTION & INNOVATION, *DFPI Moves to Suspend BlockFi's Lending License, Confirms BlockFi No Longer Lending in California* (Nov. 11, 2022), https://dfpi.ca.gov/2022/11/11/dfpi-moves-to-suspend-blockfis-lending-license-confirms-blockfi-no-longer-lending-in-california/.

[342] NEW YORK DEPARTMENT OF FINANCIAL SERVICES, *Superintendent Adrienne A. Harris Announces $100 Million Settlement with Coinbase, Inc. after DFS Investigation Finds Significant Failings in the Company's Compliance Program* (Jan. 4, 2023), https://www.dfs.ny.gov/reports_and_publications/press_releases/pr202301041.

[343] *Id.*

[344] *Id.*

falsely representing itself as a crypto exchange."[345] Under New York's Martin Act, cryptocurrency platforms are required to be registered with the State of New York.[346] Companies can register in New York by submitting registration forms and a filing fee with the State.[347] The Office of the Attorney General ("OAG") found that CoinEx and KuCoin were "able to buy and sell cryptocurrencies" on these platforms in New York, although the companies were "unregistered in the state."[348] Through these actions, the OAG "seeks to permanently stop CoinEx from operating in New York through its website and mobile apps," [349] and to "stop KuCoin from operating in New York and to block access to its website until it complies with the law."[350]

In March 2023, California's DFPI announced that crytpo lending platform BlockFi Lending LLC ("BlockFi") "agreed to direct its servicer to provide Californians more than $100,000 in refunds, subject to the bankruptcy court's approval," following a DFPI investigation that uncovered BlockFi's failure to provide timely notifications to borrowers that they could stop repaying on their BlockFi loans.[351]

Regulatory Guidance

States have also recently issued a variety of regulatory guidance and consumer-facing initiatives aimed at policing crypto-related criminal activity. In February 2023, New York's DFS announced "new enhancements" to provide "additional capabilities to detect potential insider trading, market manipulation, and front-running activity associated with Department-regulated entities' and applicants' exposure or potential exposure to listed virtual currency wallet addresses."[352]

In February 2023, California's DFPI announced the launch of its Crypto Scam Tracker,[353] which "details apparent crypto scams identified through a review of complaints submitted by the public and allows California consumers and investors to do their own research and prevent harm to themselves and others."[354]

And in March, New York's DFS announced Regulatory Guidance "to better protect customers in the event of an insolvency or similar proceeding."[355] Superintendent Adrienne A. Harris explained that this Regulatory Guidance "reminds DFS-regulated virtual currency companies of our expectations regarding the safekeeping of customer assets."[356]

State Legislative Efforts

While states have been active in enforcing existing regulations, they have also been active in proposing and enacting new ones.

---

[345] *See* NEW YORK STATE ATTORNEY GENERAL, *Attorney General James Sues Cryptocurrency Platform for Failing to Register in New York* (Feb. 22, 2023), https://ag.ny.gov/press-release/2023/attorney-general-james-sues-cryptocurrency-platform-failing-register-new-york; *see also* NEW YORK STATE ATTORNEY GENERAL, *Attorney General James Continues Crackdown on Unregistered Cryptocurrency Platforms* (Mar. 9, 2023), https://ag.ny.gov/press-release/2023/attorney-general-james-continues-crackdown-unregistered-cryptocurrency-platforms.

[346] *See* NEW YORK STATE ATTORNEY GENERAL, *Industry Alert: Registration of Commodity Brokers-Dealers, Salespersons, and Investment Advisors Doing Business Relating to Virtual or "Crypto" Currency* https://ag.ny.gov/sites/default/files/crypto-industry-notice.pdf; *see also* NEW YORK STATE ATTORNEY GENERAL, *Attorney General James Sues Cryptocurrency Platform for Failing to Register in New York* (Feb. 22, 2023).

[347] *See* NEW YORK STATE ATTORNEY GENERAL, *Broker-dealer and securities issuers registration*, https://ag.ny.gov/resources/organizations/investments-registration-regulation/broker-dealer-and-securities-issuers.

[348] NEW YORK STATE ATTORNEY GENERAL, *Attorney General James Continues Crackdown on Unregistered Cryptocurrency Platforms* (Mar. 9, 2023).

[349] NEW YORK STATE ATTORNEY GENERAL, *Attorney General James Sues Cryptocurrency Platform for Failing to Register in New York* (Feb. 22, 2023).

[350] NEW YORK STATE ATTORNEY GENERAL, *Attorney General James Continues Crackdown on Unregistered Cryptocurrency Platforms* (Mar. 9, 2023).

[351] *See* CALIFORNIA DEPARTMENT OF FINANCIAL PROTECTION & INNOVATION, *Crypto Lender BlockFi Agrees to Provide More Than $100,000 in Refunds to Californians* (Mar. 27, 2023).

[352] *See* NEW YORK DEPARTMENT OF FINANCIAL SERVICES, *DFS Superintendent Adrienne A. Harris Strengthens Department's Ability to Detect Fraud In The Virtual Currency Industry* (Feb. 21, 2023), https://www.dfs.ny.gov/reports_and_publications/press_releases/pr202302211.

[353] *See* CALIFORNIA DEPARTMENT OF FINANCIAL PROTECTION & INNOVATION, *DFPI Launches Scam Tracker to Help the Public Spot Crypto Scams* (Feb. 16, 2023), https://dfpi.ca.gov/2023/02/16/dfpi-launches-scam-tracker-to-help-the-public-spot-crypto-scams/.

[354] *Id.*

[355] *See* NEW YORK DEPARTMENT OF FINANCIAL SERVICES, *Superintendent Adrienne A. Harris Releases Consumer Protection Guidance In The Event Of Virtual Currency Insolvency* (Jan. 23, 2023), https://www.dfs.ny.gov/reports_and_publications/press_releases/pr202301231.

[356] *Id.*

Licensing Regimes

On September 23, 2022, California Governor Gavin Newsom vetoed a bill that would have strengthened crypto market regulations despite near-unanimous support from the state legislature.[357] The bill sought to establish a New York BitLicense-style regime and impose regulations on stablecoin issuers, including requirements that licensed companies only engage with bank-issued stablecoins, which in turn must remain 100% backed by reserves.[358] Governor Newsom signaled that "a more flexible approach is needed to ensure regulatory oversight can keep up with rapidly evolving technology."[359] Given the overwhelming bipartisan support, a new version of this bill was introduced on December 5, 2022 and is currently before the Appropriations Committee.[360]

In October 2022, Louisiana's Office of Financial Institutions finalized its regulations under the state's Virtual Currency Business Act.[361] The regulations, which went into effect on January 1, 2023, provide that, as of June 30, 2023, any covered entity will need a license to engage in business activity involving virtual currencies.[362] Louisiana will join a long and growing list of states that require businesses in the cryptocurrency industry to receive a license for money transmitting in order to engage in crypto transactions.

Another significant bill was introduced (although ultimately not enacted) in Hawaii. On January 24, 2022, state legislators introduced HB 2108, which would have ended the state cryptocurrency "sandbox" by requiring that crypto companies receive a license from the state before conducting transactions with Hawaii residents.[363] The bill was deferred in early May and, on June 2, the Division of Financial Institutions announced a two-year extension of the Digital Currency Innovation Labe program, thus extending the sandbox.[364] Hawaii might reevaluate its position after the extension period, but for participants in the sandbox program, no license will be needed until at least June 30, 2024.

Taxes

State legislators in California also introduced a bill to join Wyoming and Arizona in proposing legislation to allow payment of state taxes via cryptocurrency. On February 18, 2022, SB 1275 was introduced in the California Senate to authorize state agencies to accept cryptocurrency as a method of payment for government services.[365] While SB 1275 failed to pass committee on April 5, it signals persistent interest in integrating cryptocurrency into public works. As this continues, the intermingling of public projects, taxes, and cryptocurrency will lead to heightened compliance regulations around tax reporting, anti-money laundering, and cybersecurity.

The Arizona legislature passed SB 1236, which "barred local authorities in Arizona from imposing taxes on the use of blockchain nodes or the technology used to mine digital assets."[366] Governor Katie Hobbs vetoed the bill in April 2023 because it too "broadly defines' blockchain technology' and prevents local policymaking concerning an emergent and potentially energy-intensive economic activity."[367] Nonetheless, this bill highlights the tension between

---

[357] *See* CALIFORNIA OFFICE OF GOVERNOR, *September 23, 2022 Statement to Members of the California State Assembly*, https://www.gov.ca.gov/wp-content/uploads/2022/09/AB-2269-VETO.pdf.

[358] *See* Assem. Bill 2269, 2021-2022, 1st. Ex. Sess., (CA. 2022), https://leginfo.legislature.ca.gov/faces/billTextClient.xhtml?bill_id=202120220AB2269.

[359] *See* CALIFORNIA OFFICE OF GOVERNOR, *September 23, 2022 Statement to Members of the California State Assembly*.

[360] *See* Assem. Bill 2269, 2021-2022, 1st. Ex. Sess., (CA. 2022); *see also* Titus Wu, Crypto Rule Push in California Sees Momentum After FTX Debacle, BLOOMBERG TAX (Jan. 23, 2023), https://news.bloombergtax.com/crypto/crypto-rule-push-in-california-sees-momentum-after-ftx-debacle.

[361] *See* LOUISIANA OFFICE OF FINANCIAL INSTITUTIONS, *Declaration of Emergency Regarding Virtual Currency Business Activity*, http://www.ofi.state.la.us/NonDepVirtualCurrencyBusinessEmergencyRule_LAC_10_I_1901_et_seq.pdf.

[362] *Id.*

[363] *See* H.B. 2108, 2022 Leg., (Haw. 2022), https://www.capitol.hawaii.gov/session/archives/measure_indiv_Archives.aspx?billtype=HB&billnumber=2108&year=2022.

[364] *Se ge* Ellen Ng, State of Hawai'i's Digital Currency Innovation Lab Extended to June 30, 2024, HTDC (June 2, 2022) https://www.htdc.org/state-of-hawaiis-digital-currency-innovation-lab-extended-to-june-30-2024/.

[365] *See* Assem. Bill 1275, 2021-2022, 1st Ex. Sess., (Ca. 2022), https://leginfo.legislature.ca.gov/faces/billPdf.xhtml?bill_id=202120220SB1275&version=20210SB127599INT.

[366] *See* Steve Kaaru, Arizona governor vetoes bill offering tax reprieve for miners, COINGEEK (Apr. 17, 2023), https://coingeek.com/arizona-governor-vetoes-bill-offering-tax-reprieve-for-miners/.

[367] ARIZONA OFFICE OF THE GOVERNOR, *April 12, 2023 Statement to the Members of the State Senate,* https://azgovernor.gov/sites/default/files/veto_letter_sb1236_0_0_0.pdf.

local policy makers in a still-fluid digital asset marketplace.

On the other hand, in March 2023, Oklahoma advanced legislation that would "extend a tax break to bitcoin and cryptocurrency miners that set up shop" in the state.[368] Other states, like Illinois and Georgia are considering similar measures, and Kentucky has already approved tax incentives for bitcoin miners as of April 2022.[369]

Stable Coin Regulations

Following the collapse of TerraUSD, on June 8, 2022, the New York DFS issued guidance for stablecoin issuers in New York.[370] DFS advised that stablecoins must be fully backed by a reserve of assets, the assets must be separated from the proprietary assets of the issuing entity, and the reserves must be subject to examination at least once a month by a CPA.[371] DFS also highlighted its concern with other risks such as cybersecurity, network design and maintenance, and compliance with the Bank Secrecy Act and anti-money laundering statutes.[372] This guidance underscores two trends: (1) the cryptocurrency industry is under a microscope when it comes to compliance with cybersecurity, data privacy, and consumer protection regulatory regimes, and (2) there is a growing desire from state legislators to have all stablecoins supported by a 1-to-1 ratio of reserves on hand.

Wyoming has continued to be at the forefront of state crypto regulatory regimes. On February 17, 2022, a bipartisan group of state lawmakers introduced SF 0106 which would authorize the state treasurer to issue "Wyoming stable tokens," while also creating an oversight committee to engage in independent auditing of the program.[373] The Governor vetoed the bill on March 25, 2022,[374] however, there continues to be bipartisan interest in further exploring legislation in this area. If passed in upcoming legislative cycles, Wyoming would be the first state to have its own stablecoin, which could lead to increased regulations around the use of the stablecoin in cryptocurrency transactions.

Cryptocurrency Mining

On November 20, 2022, New York became the first state to enact a two-year moratorium on new cryptocurrency mining permits at fossil fuel plants.[375] SB 6486D prohibits crypto companies from retrofitting outdated fossil fuel plants to serve as crypto mining facilities as a move aimed to address climate concerns over the energy-intensive crypto mining activity.[376] The legislation also provides that any future cryptocurrency mining operations will be subject to "a full generic environmental impact statement review."[377]

Encouraging Innovation

States have also attempted to issue more comprehensive legislation aimed at fostering innovation in the digital asset space. New Jersey Senate Bill 1756[378] and Assembly Bill 2371[379] propose the Digital Asset and Blockchain Technology Act, which would "allow decentralized autonomous organizations to form in the state, allow companies to issue electronic stock certificates, and create tax incentives for virtual currency businesses to move to New Jersey," while also requiring "developers to file online with the Department of Banking and Insurance before making an open blockchain token available for

---

[368] *See* Michael McSweeney, Oklahoma joins widening group of US states mulling tax incentives for bitcoin miners, THE BLOCK (Apr. 13, 2022), https://www.theblock.co/linked/140343/oklahoma-joins-widening-group-of-us-states-mulling-tax-incentives-for-bitcoin-miners.

[369] *Id.*

[370] *See* NEW YORK DEPARTMENT OF FINANCIAL SERVICES, *Guidance on the Issuance of U.S. Dollar-Backed Stablecoins* (June 8, 2022), https://www.dfs.ny.gov/industry_guidance/industry_letters/il20220608_issuance_stablecoins#:~:text=The%20stablecoin%20must%20be%20fully,end%20of%20each%20business%20day..

[371] *Id.*

[372] *Id.*

[373] *See SF 0106, Wyoming Stable Token Act*, 2022 Leg., (Wyo. 2022), https://wyoleg.gov/Legislation/2022/SF0106?source=email.

[374] *See* Wyoming Legislature, *Veto of SEA0050/SF0106 - Wyoming Stable Token Act* (Mar. 25, 2022), https://wyoleg.gov/2022/Veto/SF0106.pdf.

[375] *See Senate Bill S6486D Signed by Governor*, 2021-2022 Leg., (N.Y. 2022), https://www.nysenate.gov/legislation/bills/2021/S6486.

[376] *Id.*

[377] *Id.*

[378] S1756, 2021-2022 Leg. (N.J. 2022), https://www.njleg.state.nj.us/bill-search/2022/S1756/bill-text?f=S2000&n=1756_R1.

[379] A2371 AcaSca (2R), 2022-2023 Leg. (N.J. 2023), https://www.njleg.state.nj.us/bill-search/2022/A2371.

sale and pay a $1,000 filing fee."[380] The sponsors claim this Act "will strike a better balance of encouraging innovation while simultaneously protecting investors–something New York's regulatory framework is historically criticized for."[381]

Other states are wary of federally controlled digital assets and have put forth legislation to that effect. In March 2023, Governor of Florida Ron DeSantis announced "comprehensive legislation" to protect "consumers and businesses from a federally controlled" Central Bank Digital Currency ("CBDC").[382] Governor DeSantis's proposal would "[e]xpressly prohibit[] the use of a federally adopted Central Bank Digital Currency as money within Florida's Uniform Commercial Code" and "[i]nstitut[e] protections against a central global currency by prohibiting any CBDC issued by a foreign reserve or foreign sanctioned central bank."[383]

* * *

King & Spalding's global Fintech, Blockchain and Cryptocurrency Group provides seamless coordination across countries and jurisdictions and is a "one-stop" shop for fintech clients pursuing strategic transactions, regulatory compliance and litigation matters. Our attorneys are experienced at working with fintech companies across a variety of industry segments, including peer-to-peer and alternative lending, digital currency and blockchain technology, and mobile and online payments.

[380] Jessica Livingston & Felix Shipkevich, New Jersey Legislation to Regulate Virtual Currencies Likely to Become Law, JDSUPRA (Feb. 27, 2023), https://www.jdsupra.com/legalnews/new-jersey-legislation-to-regulate-1011684/.
[381] *Id.*
[382] FLORIDA GOVERNOR'S OFFICE, *Governor Ron DeSantis Announces Legislation to Protect Floridians from a Federally Controlled Central Bank Digital Currency and Surveillance State* (Mar. 20, 2023), https://www.flgov.com/2023/03/20/governor-ron-desantis-announces-legislation-to-protect-floridians-from-a-federally-controlled-central-bank-digital-currency-and-surveillance-state/.
[383] *Id.*

Contributors

J.C. Boggs
Partner
jboggs@kslaw.com

Andrew Michaelson
Partner
amichaelson@kslaw.com

Daniel Kahan
Partner
dkahan@kslaw.com

Ehren Halse
Partner
ehalse@kslaw.com

Shas Das
Counsel
sdas@kslaw.com

Danielle Pressler
Counsel
dpressler@kslaw.com

Luke Roniger
Senior Associate
lroniger@kslaw.com

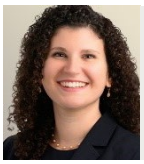
Kyle Maury
Associate
kmaury@kslaw.com

Diana Liu
Associate
dliu@kslaw.com

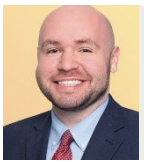
Read Mills
Associate
rmills@kslaw.com

John Morrison
Associate
jmorrison@kslaw.com

Karina Houghton
Associate
khoughton@kslaw.com



Lauren Konczos
Associate
lkonczos@kslaw.com



Hunter McGhee
Associate
hmcghee@kslaw.com

Spencer Young
Law Clerk
syoung@kslaw.com

Anna Romanova
Associate
aromanova@kslaw.com

Gladys Morales
Associate
gmorales@kslaw.com