United States Government Accountability Office

Report to Congressional Requesters

June 2023

BLOCKCHAIN IN FINANCE

Legislative and Regulatory Actions Are Needed to Ensure Comprehensive Oversight of Crypto Assets

GAO-23-105346

GAO Highlights

Highlights of GAO-23-105346, a report to congressional requesters

Why GAO Did This Study

Blockchain-related financial products and services have grown substantially in recent years. For example, crypto assets reached a peak market capitalization of nearly $3 trillion in November 2021. However, recent volatility, bankruptcies, and instances of fraud in these markets illustrate the harm consumers and investors may face without adequate protections. Regulators and industry stakeholders are concerned regulatory gaps may limit regulators' ability to address risks these products and services pose. Modernizing the financial regulatory system is on GAO's high-risk list, partly because some entities are not subject to comprehensive regulation.

GAO was asked to study the regulation of blockchain-related financial products and services. Among other objectives, this report examines regulatory gaps and coordination in regulating these applications. GAO reviewed and analyzed government and industry reports, government guidance and speeches, and laws and regulations. GAO interviewed agency officials and market participants and observers.

What GAO Recommends

GAO recommends Congress consider legislation for federal oversight of nonsecurity crypto asset spot markets and stablecoins. GAO is also making seven recommendations (one to each of seven financial regulators) to establish a (or adapt an existing) coordination mechanism to identify and address blockchain-related risks. One regulator agreed with the recommendation and the others neither agreed nor disagreed.

View GAO-23-105346. For more information, contact Michael E. Clements at (202) 512-8678 or clementsm@gao.gov.

June 2023

BLOCKCHAIN IN FINANCE

Legislative and Regulatory Actions Are Needed to Ensure Comprehensive Oversight of Crypto Assets

What GAO Found

Blockchain allows users to conduct and record tamper-resistant transactions that multiple parties make without a central authority, such as a bank, when used for financial transactions. Because of these characteristics, blockchain-related products and services have the potential to produce cost savings, faster transactions, and other benefits over their traditional counterparts. However, these benefits have not been fully realized. Furthermore, the significant risks these products pose have been realized and negatively affected consumers and investors. For example, crypto assets have experienced price volatility. Also, the bankruptcy of FTX Trading Ltd., a prominent crypto asset trading platform, led to the discovery that a substantial portion of the platform's assets might be missing or stolen, according to bankruptcy-related documents.

GAO found gaps in regulatory authority over two blockchain-related products that raise consumer and investor protection and financial stability concerns.

- No federal financial regulator has comprehensive authority to regulate the spot market for crypto assets that are not securities. In contrast, platforms that trade crypto asset securities and operate as exchanges as defined by federal securities laws are subject to registration and regulation as national securities exchanges, unless an exemption applies. Several platforms without federal oversight have experienced fraud and trading manipulation. By providing for more comprehensive oversight of these platforms, Congress could better ensure users' protection from unfair and manipulative trading practices.
- Gaps in regulatory authority exist in the oversight of stablecoins (a crypto asset purported to hold a stable value relative to a fiat currency, such as the U.S. dollar). To keep their value, issuers often state their stablecoins are backed by reserve assets. But no uniform standards exist for reserve levels and risks or for public disclosure of reserves. This increases the risk that a stablecoin may not be able to hold its value and honor user redemption requests. To the extent these stablecoins become more integrated into the financial system, their failures could pose risks to financial stability. By providing for consistent and comprehensive oversight of stablecoins, Congress could better ensure protections for consumers, investors, and the financial system.

Regulators lack an ongoing coordination mechanism for addressing blockchain risks in a timely manner. For example, regulators identified financial stability risks posed by stablecoins in 2019, but they did not identify the need for Congressional action to address the risks until November 2021 (in a report issued through the President's Working Group on Financial Markets). A formal coordination mechanism for addressing blockchain-related risks, which could establish processes or time frames for responding to risks, could help federal financial regulators collectively identify risks and develop timely and appropriate responses. In turn, this could improve protections for consumers and investors, mitigate illicit finance and threats to financial stability, and promote responsible innovation and U.S. competitiveness.

Contents

Abbreviations

AML	anti-money laundering
BSA	Bank Secrecy Act
CFPB	Consumer Financial Protection Bureau
CFTC	Commodity Futures Trading Commission
DeFi	decentralized finance
Dodd-Frank Act	Dodd-Frank Wall Street Reform and Consumer Protection Act
FDIC	Federal Deposit Insurance Corporation
Federal Reserve	Board of Governors of the Federal Reserve System
FinCEN	Financial Crimes Enforcement Network
FINRA	Financial Industry Regulatory Authority Inc.
FSOC	Financial Stability Oversight Council
FTX	FTX Trading Ltd.
NCUA	National Credit Union Administration
OCC	Office of the Comptroller of the Currency
OFR	Office of Financial Research
PWG	President's Working Group
SEC	Securities and Exchange Commission

U.S. GOVERNMENT ACCOUNTABILITY OFFICE
441 G St. N.W.
Washington, DC 20548

June 22, 2023

The Honorable Maxine Waters
Ranking Member
Committee on Financial Services
House of Representatives

The Honorable Stephen F. Lynch
Ranking Member
Subcommittee on Digital Assets, Financial Technology and Inclusion
Committee on Financial Services
House of Representatives

Blockchain allows users to conduct and record transfers of crypto assets without a central authority, such as a bank.[1] Markets for financial products and services using blockchain technology have grown enormously in recent years. For example, crypto assets reached a peak market capitalization of nearly $3 trillion in November 2021, according to one estimate.[2]

Proponents of crypto assets suggest financial products and services based on blockchain have the potential to reduce costs and improve access to the financial system. However, recent turmoil in crypto asset markets resulted in heavy losses to crypto asset holders, and several prominent crypto asset platforms filed for bankruptcy protection.[3] For example, crypto asset trading platform FTX Trading Ltd. (FTX), which has

[1]For the purpose of this report, a crypto asset is a private-sector digital instrument that primarily depends on cryptography and distributed ledger technology or similar technology as defined by the Financial Stability Board. Ledgers are “distributed” because multiple participants in a computer network share and synchronize copies of the ledger. See Financial Stability Board, *Assessment of Risks to Financial Stability from Crypto-assets* (Basel, Switzerland: Feb. 16, 2022).

[2]Total crypto asset market capitalization tracks the value of all crypto assets and is calculated by multiplying the prices of crypto assets by their circulating supplies, according to Coinmarketcap.com.

[3]According to Coinmarketcap.com, the total market capitalization for crypto assets declined by around 73 percent from November 2021 to June 2022 (to about $800 billion). After rebounding slightly to just over $1 trillion, market capitalization declined to under $800 billion in November 2022 in the wake of further market turmoil. As of June 5, 2023, the market capitalization for crypto assets was about $1.1 trillion.

filed for U.S. bankruptcy court protection, reported that it owes its 50 largest creditors nearly $3.1 billion.

Some federal financial regulators and industry observers have expressed concerns that consumers and investors may not fully understand the risks of blockchain-related products and services or have adequate protections.[4] They also have expressed concerns about regulators' authority to comprehensively address these risks.

We previously reported that the U.S. financial regulatory structure is fragmented, with state and federal regulators having overlapping responsibilities for different types of financial institutions.[5] In 2009, we added modernizing the U.S. financial regulatory system to our high-risk list, partly because entities with critical roles in the financial markets were not subject to sufficiently comprehensive regulation and oversight, and because the regulatory system was not effectively providing key information and protections to consumers and investors for new and complex financial products.[6] We also previously reported that the current financial regulatory framework may deter innovation in blockchain-related products or result in firms moving their blockchain-related products to jurisdictions with greater regulatory clarity.[7]

You asked us to examine the regulatory framework for the use of blockchain in the financial sector. This report examines (1) key blockchain-related products and services in financial services, including their potential benefits and risks; (2) federal financial regulators' jurisdiction over blockchain-related products and services; (3) gaps in

[4]In this report, we discuss the following federal financial regulators—Commodity Futures Trading Commission, Securities and Exchange Commission, Federal Deposit Insurance Corporation, Board of Governors of the Federal Reserve System, Office of the Comptroller of the Currency, Consumer Financial Protection Bureau, and National Credit Union Administration—as well as entities in the Department of the Treasury (Financial Stability Oversight Council and Financial Crimes Enforcement Network) that have oversight authorities relating to systemic risk and illicit finance, respectively.

[5]GAO, *Financial Regulation: Complex and Fragmented Structure Could Be Streamlined to Improve Effectiveness*, GAO-16-175 (Washington, D.C.: Feb. 25, 2016).

[6]The High-Risk List highlights federal programs and operations that we have determined are in need of transformation and names federal programs and operations that are vulnerable to waste, fraud, abuse, and mismanagement. See GAO, *High-Risk Series: Dedicated Leadership Needed to Address Limited Progress in Most High-Risk Areas*, GAO-21-119SP (Washington, D.C.: Mar. 2, 2021).

[7]GAO, *Blockchain: Emerging Technology Offers Benefits for Some Applications but Faces Challenges*, GAO-22-104625 (Washington, D.C.: Mar. 23, 2022).

regulatory authority; and (4) regulators' coordination on and response to risks posed by blockchain-related products and services.

For the first objective, we reviewed and analyzed prior GAO reports and reports from federal financial regulators, international financial regulatory associations, and industry associations representing banks and blockchain-related financial service companies.

For the second objective, we reviewed and analyzed prior GAO reports; relevant laws and regulations; and federal financial regulator reports, guidance, speeches, and enforcement actions.

For the third objective, we reviewed relevant laws and regulations; proposed legislation; Congressional Research Service reports; federal financial regulator reports, studies, guidance, speeches, and enforcement actions; and studies from international financial regulatory bodies. We focused our analysis on three blockchain-related products and services: platforms for trading crypto assets, stablecoins (a type of crypto asset that purports to mitigate price volatility), and decentralized finance—known as DeFi—which aims to automate financial transactions through computer code. We chose these three products and services because of their rapid growth, exposure to retail customers, and their potential risks, among other factors.

For the fourth objective, we reviewed federal financial regulator reports, guidance, speeches, and enforcement actions; recent Executive Orders; and information obtained from our regulatory gap analyses for the third objective.

For both the third and fourth objectives, we assessed the information obtained against GAO's 2009 framework for crafting and assessing proposals to modernize the U.S financial regulatory system.[8]

For all four objectives, we interviewed officials from the following federal financial regulatory agencies—Consumer Financial Protection Bureau (CFPB), Commodity Futures Trading Commission (CFTC), Federal Deposit Insurance Corporation (FDIC), Board of Governors of the Federal

[8]GAO, *Financial Regulation: A Framework for Crafting and Assessing Proposals to Modernize the Outdated U.S. Financial Regulatory System*, GAO-09-216 (Washington, D.C.: Jan. 8, 2009). To develop this framework, we synthesized existing GAO work and other studies and met with dozens of representatives of financial regulatory agencies, industry associations, consumer advocacy organizations, and other organizations.

Reserve System (Federal Reserve), National Credit Union Administration (NCUA), Office of the Comptroller of the Currency (OCC), and Securities and Exchange Commission (SEC). We also interviewed officials from the following entities and offices in the Department of the Treasury—Financial Crimes Enforcement Network (FinCEN), Financial Stability Oversight Council (FSOC), Office of Domestic Finance, and Office of Financial Research (OFR).

We also interviewed officials of two self-regulatory organizations, three state regulatory associations, and state financial regulatory agencies in Wyoming and New York (chosen because they have explicit laws and regulations for certain crypto asset activities). Additionally, we interviewed consumer advocacy organizations, industry associations representing banking and traditional and blockchain-related financial services companies, and a crypto industry research and advocacy organization. Finally, we conducted three group discussions with a nonrandom selection of 10 firms offering or representing crypto asset trading platforms, stablecoin issuers, and DeFi companies (one discussion group for each category), representing a range of business models. See appendix I for more details on our scope and methodology.

We conducted this performance audit from July 2021 to June 2023 in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

Background

Blockchain

Blockchain is a type of distributed ledger.[9] Its core function is to create a tamper-resistant ledger that records transactions in crypto assets. A blockchain ledger is considered tamper-resistant because it uses cryptographic means to validate transactions and the data on ownership and transfer of these assets is viewable across many computers and users. This structure reduces the likelihood that a single failure or

[9]Distributed ledgers are tools that allow users to conduct and record transfers of digital assets without a central authority. They are “distributed” because multiple participants in a computer network (individuals, businesses, etc.) share and synchronize copies of the ledger.

dishonest user could compromise network integrity or tamper with the information recorded on the blockchain.

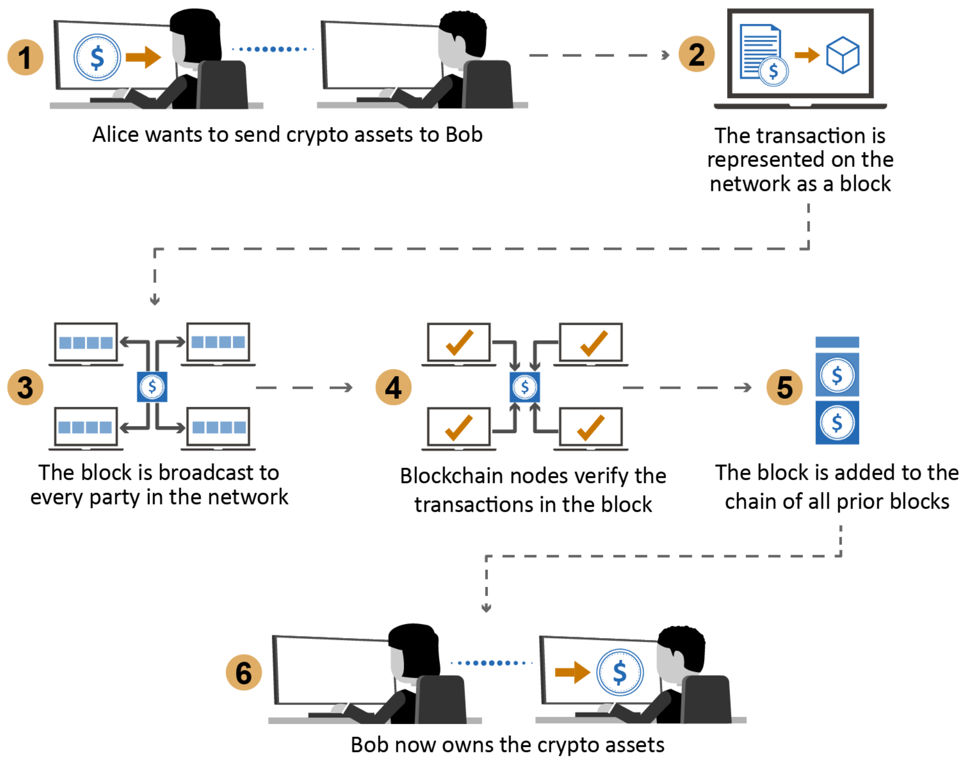
Blockchains do not require a central authority, unlike centralized databases used in traditional financial services. This decentralization is possible because blockchain (1) uses cryptographic techniques to computationally verify transactions and (2) builds a tamper-resistant ledger. This involves cryptographically "chaining" a grouping of newly added data—known as a block—to previous blocks. This process prevents changes unless they are verified by other users.[10]

Overview of Blockchain Transactions

Each blockchain transaction, such as a transfer of a crypto asset between two parties, is written to the blockchain. Users' crypto asset balances are associated with crypto asset addresses that use principles of cryptography to help safeguard against inappropriate tampering. When users transfer crypto assets, the recipient provides their crypto asset address to the sender, and the sender authorizes the transaction with their private key (essentially a secret code that proves the sender's control over their crypto asset address). See figure 1 for an illustration of a simplified crypto asset transaction.

[10] GAO-22-104625.

Figure 1: Simplified Example of Blockchain Operation to Send Crypto Assets



Source: GAO. | GAO-23-105346

Users may store components of crypto asset transactions such as private keys and addresses in a virtual wallet, which allows them to access their crypto assets. Crypto asset wallets can be custodial or noncustodial. With a custodial wallet, a service provider (such as a crypto asset trading platform or third-party wallet provider) holds the users' private keys. Holding the users' private keys enables the custodial wallet provider to exercise full control over the user's assets, although the custodian generally will have contractual or other legal obligations to take direction from the user regarding the assets, such as sending a remittance or making a payment. A noncustodial wallet is located on the user's computer or other data storage device, and the user retains full control over the private keys and the assets in the wallet.

Through blockchain, users share data directly with other users through networks of interconnected computer systems and conduct permitted activities without a central server or intermediary, in what is known as a peer-to-peer network. The transactions do not require the disclosure of information about a user's identity, giving participants some degree of anonymity. However, in some cases the transactions are not completely anonymous because certain information about a transaction, such as the time and amount of each transaction and the associated crypto asset addresses are permanently recorded in the blockchain.[11] As a result, peer-to-peer crypto asset transactions are sometimes described as "pseudonymous."

Types of Blockchains

Blockchains can be divided into two categories:

- Permissionless blockchains are open to everyone to contribute data. Anyone has the right to read and engage in transactions on a permissionless blockchain. Because permissionless blockchain networks are open, malicious users may attempt to publish blocks in a way that subverts the system. To help prevent this, such networks often use a consensus protocol that requires users to expend or maintain resources when attempting to publish blocks.[12] This requirement usually promotes nonmalicious behavior by rewarding the successful publishers of blocks with the blockchain's "native" crypto assets.
- Permissioned blockchains are privately operated, and only specified entities (authorized users) are allowed to access the network and engage in transactions.

Smart Contracts

Smart contracts are a tool to extend the functionality of a blockchain beyond recording transactions, although not all blockchains support them. Smart contracts consist of code and data that can automatically run on the blockchain using cryptographically signed transactions. They are used to automatically transfer crypto assets on the blockchain if certain conditions are met. These conditions can include those relating to payment terms, liens, confidentiality, and enforcement. Smart contracts also can provide services such as collecting input data from external sources and making decisions based on that information. To be a legally

[11]While popular crypto assets such as Bitcoin record transactions on public blockchain ledgers, some blockchains have embedded privacy technology that limits what can be viewed on the ledger. For example, privacy coins such as Monero offer enhanced encryption features that make it more difficult to trace or attribute transactions.

[12]Consensus protocols are the steps a blockchain takes to ensure verified blocks are added to the ledger and unverified blocks are ignored. It is the way in which at least a majority of blockchain network members agree on the information of a proposed transaction, which is then written to the ledger.

binding contract, a smart contract generally must meet all requirements imposed by law.

Financial Regulatory Structure

The U.S. financial regulatory structure is fragmented among multiple agencies with varying primary missions that include safety and soundness oversight, securities and derivatives markets oversight, illicit finance oversight, and consumer protection oversight. Additionally, the Dodd-Frank Wall Street Reform and Consumer Protection Act (Dodd-Frank Act) created FSOC to provide for systemic risk oversight.[13]

Safety and Soundness Oversight of Depository Institutions

Safety and soundness (also known as prudential) oversight encompasses the health of a financial institution, such as capital and liquidity levels. Four federal banking regulators—the Federal Reserve, OCC, FDIC, and NCUA—as well as state banking regulators oversee their respective depository institutions for safety and soundness (see table 1).[14] The banking regulators establish capital, liquidity, and other requirements; conduct on-site examinations and off-site monitoring to assess an institution's financial condition, operational security, and governance; and monitor compliance with applicable laws and regulations. They also have the authority to take enforcement actions against noncompliant depository institutions under their jurisdiction.

Table 1: Federal Prudential Regulators and Their Basic Functions

Agency	Basic function
Office of the Comptroller of the Currency	Charters and supervises national banks, federal thrifts, and federally chartered branches and agencies of foreign banks.
Board of Governors of the Federal Reserve System	Supervises state-chartered banks that opt to be members of the Federal Reserve System, bank and thrift holding companies and their nondepository subsidiaries and nonbank financial companies designated by the Financial Stability Oversight Council for consolidated supervision and enhanced prudential standards. Supervises the U.S. operations of foreign banking organizations, and Edge Act and agreement corporations.
Federal Deposit Insurance Corporation	Supervises state-chartered banks that are not members of the Federal Reserve System, as well as state savings banks and thrifts; insures the deposits of all banks and thrifts that are approved for federal deposit insurance; has the authority to conduct backup examinations for any insured institution; resolves all failed insured banks and thrifts; and, if appointed receiver by the Secretary of the Treasury, has authority to resolve certain large bank holding companies and nonbank financial companies.

[13]Pub. L. No. 111-203, §§ 111-123,124 Stat. 1376, 1392-1412 (2010) (codified as amended at 12 U.S.C. §§ 5321-35).

[14]For purposes of this report, unless otherwise indicated, we use "banks" generally to refer to both banks and credit unions, and "federal banking regulators" to include NCUA.

Agency	Basic function
National Credit Union Administration	Charters and supervises federally chartered credit unions and insures savings in federal and most state-chartered credit unions.

Source: GAO. | GAO-23-105346

Securities and Derivatives Markets Oversight

SEC and CFTC regulate the securities and commodity derivatives markets, under a combination of direct oversight and oversight of self-regulatory organizations that oversee market participants.[15] State securities regulators also play a role in overseeing the securities markets.

SEC's mission is to protect investors; maintain fair, orderly, and efficient markets; and facilitate capital formation. SEC has jurisdiction over entities, transactions, and other activities that involve assets that meet the definition of securities under the federal securities laws, including securities derivatives.[16] In determining whether an asset is subject to its regulation, SEC looks to see whether the asset meets the statutory definition of a "security" under the federal securities laws. One type of security is an "investment contract." SEC often applies the *Howey* test, which was set forth by the Supreme Court (and subsequent case law), to

[15]The federal securities laws define the term security to include an investment contract, as well as other instruments such as notes, stocks, bonds, and transferable shares. 15 U.S.C. §§ 77b(a)(1); 78c(a)(10). Commodity derivatives are contracts or financial instruments that derive their value from an underlying measure, such as the price of an asset—where the underlying asset or other measure falls within the definition of commodity under the Commodity Exchange Act. 7 U.S.C. §§ 1-27f. CFTC regulatory authority generally includes the markets on which commodity options and futures trade and broad authority over the swap markets.

[16]SEC has the authority to regulate security-based swaps. "Swaps" are financial contracts in which two counterparties agree to exchange or swap payments with each other as result of changes in things like a stock price, interest rate or commodity price. The Dodd-Frank Act gave CFTC the authority to regulate "swaps" and SEC the authority to regulate "security-based swaps" which are swaps based on securities. Security-based swaps include swaps based on narrow-based security indexes, a single security or loan or any interest therein or any value thereof, or the occurrence or non-occurrence of certain financial events related to issuers of securities. *See* 15 U.S.C. 78c(a)(68)(A). Swaps that have features of both swaps and security-based swaps are known as "mixed-swaps" and are governed by both CFTC and SEC. *See* 15 U.S.C. § 78c(a)(68)(D); 7 U.S.C. § 1a(47)(D).

determine whether a crypto asset is a security under federal securities laws.[17]

The federal securities laws require registration of offers and sales of securities to the public unless an exemption applies. Broker-dealers that facilitate transactions in securities, are required to register with SEC and become members of the Financial Industry Regulatory Authority Inc. (FINRA).[18] Securities exchanges that constitute the secondary market for securities, and funds that invest in them for the benefit of their shareholders are also regulated.

In regulating the securities markets, SEC establishes and maintains standards to promote market integrity—that is, to promote fair, orderly, and efficient markets, prevent fraud, and safeguard securities and funds. For example, SEC requires full disclosure of material information from issuers of securities and public companies so that investors and other market users can make informed decisions. SEC may bring enforcement actions against individuals and entities for fraud, financial and accounting irregularities and misstatements, failure to register as required, and other misconduct.

CFTC's mission is to deter and prevent price manipulation or any other disruptions to market integrity; protect market users and the public from fraud, abusive practices, and systemic risk; and foster open, competitive, and financially sound derivatives markets. CFTC has jurisdiction over the markets for commodity derivatives. Public markets for derivatives

[17]The Supreme Court's *Howey* test is used with subsequent case law to determine whether certain transactions are investment contracts. The test generally deems a financial instrument an "investment contract" if it involves an investment of money in a common enterprise with the expectation of profits to be derived from the managerial or entrepreneurial efforts of others. *SEC v. W.J. Howey Co*., 328 U.S. 293, 298-99 (1946). SEC also has applied factors set out in *Reves v. Ernst & Young*, 494 U.S. 56 (1990) in enforcement actions to determine if a financial instrument is a "note" that is a security under the federal securities laws. *See* BlockFi Lending LLC, Securities Act Rel. No. 11029, Investment Company Act Rel. No. 34503, SEC File No. 3-20758, 2022 WL 462445 (Feb. 14, 2022).

[18]FINRA is a self-regulatory organization registered with SEC as a national securities association. All securities broker-dealers doing business with the public in the United States must be registered with FINRA. FINRA writes rules to govern these firms and their representatives, and examines for and enforces broker-dealer compliance with FINRA rules and federal securities laws. SEC oversees FINRA and its rules are subject to approval by SEC.

primarily consist of contracts for future delivery (known as futures contracts), options on futures contracts, and, to a limited extent, swaps.[19]

CFTC regulation of the derivatives markets focuses on protecting price and market integrity, so that the derivatives perform as expected. CFTC requires registration from and regulates market participants that transact with derivatives, such as entities (called futures commission merchants) that buy and sell them on behalf of clients, and derivatives exchanges that constitute the secondary market for them (called designated contract markets).[20] CFTC may take enforcement action in certain situations (such as buyers or sellers manipulating market prices and undermining the integrity of the derivatives markets).

CFTC does not directly regulate the markets trading the commodities underlying derivatives contracts, known as "spot" (or cash) commodity markets.[21] However, CFTC has anti-fraud and anti-manipulation

[19]Many derivatives (primarily swaps and options) are privately negotiated between two parties. But the parties often refer to prices and other public market activities to determine the terms of their derivatives. CFTC may regulate the activities of the parties engaged in these private negotiations through registration and other requirements.

[20]In general, a futures commission merchant solicits or accepts orders for commodities futures, commodity options, or swaps, among other things, and accepts any money, securities, or property to margin, guarantee, or secure any trades or contracts that result therefrom. *See* 7 U.S.C. § 1a(28). Futures commission merchants generally must be members of the National Futures Association. 17 C.F.R. § 170.15.

[21]A cash commodity is the physical or actual commodity as distinguished from the futures contract, and is sometimes called a spot commodity. The Commodity Exchange Act subjects certain retail commodity transactions conducted with margin, leverage, or other financing to Commission oversight. The Act provides that such transactions are subject to sections 4(a), 4(b), and 4b of the Act as if the transactions were futures contracts. 7 U.S.C. § 2(c)(2)(D)(iii). A retail commodity transaction may be excepted from this section if actual delivery of the commodity occurs within 28 days of the transaction or such longer period as the CFTC may determine. 7 U.S.C. § 2(c)(2)(D)(ii)(III)(aa). *See* Retail Commodity Transactions Involving Certain Digital Assets, 85 Fed. Reg. 37734 (June 24, 2020).

enforcement authority over sales of commodities in interstate commerce, including spot transactions.[22]

Consumer Protection Oversight

Consumer protection oversight generally involves ensuring that consumers have access to markets for consumer financial products and services and that these markets are fair, transparent, and competitive. CFPB generally regulates the offering and provision of consumer financial products and services under federal consumer financial law, including the prohibition on unfair, deceptive, or abusive acts or practices.[23] This generally includes broad rulemaking, examination, and enforcement authorities.[24] Specifically for insured depository institutions with more than $10 billion in total assets, and their affiliates, CFPB has exclusive authority to examine for (and primary authority to enforce) compliance with federal consumer financial law.[25] CFPB likewise has authority to examine certain nonbanks—such as mortgage originators and servicers, payday lenders, and private student lenders—for compliance with federal consumer financial law.[26] CFPB also has certain authorities over service providers to the aforementioned entities.

Federal banking regulators have supervisory and enforcement authority for federal consumer financial law in relation to insured depository institutions with assets of $10 billion or less. They also have authority for

[22]The Commodity Exchange Act makes it unlawful for any person to use or employ in connection with any "contract of sale of any commodity in interstate commerce, or for future delivery on or subject to the rules of any registered entity, any manipulative or deceptive device or contrivance, in contravention of such rules and regulations as the [CFTC] shall promulgate" 7 U.S.C. § 9(1). CFTC regulations make it unlawful for any person, in connection with any contract of sale of any commodity in interstate commerce to intentionally or recklessly "[u]se or employ, or attempt to use or employ, any manipulative device, scheme, or artifice to defraud." 17 C.F.R. § 180.1.

[23]Federal consumer financial law includes Title X of the Dodd Frank Wall Street Reform and Consumer Protection Act, the Electronic Fund Transfer Act, Equal Credit Opportunity Act, Truth in Lending Act, Fair Debt Collection Practices Act, and certain other consumer financial protection laws, as well as regulations issued thereunder. 12 U.S.C. §§ 5481(12), 5481(14). The Bureau's authorities are subject to certain limitations. 12 U.S.C. §§ 5517, 5519.

[24]12 U.S.C. §§ 5512-5516, §§ 5561-5567.

[25]12 U.S.C. § 5515.

[26]12 U.S.C. § 5514.

certain consumer protection laws for institutions with more than $10 billion in total assets.

Illicit Finance Oversight

FinCEN administers Bank Secrecy Act (BSA) and related anti-money laundering (AML) regulations and has authority to enforce compliance with BSA.[27] BSA and its implementing regulations generally require financial institutions to assist government agencies in detecting and preventing money laundering and terrorist financing by establishing and maintaining compliance programs, conducting ongoing monitoring of customers and transactions, and identifying and reporting suspicious activity. If warranted, these institutions file suspicious activity reports.[28]

Systemic Risk Oversight

FSOC's statutory purposes include identifying risks to U.S. financial stability, promoting market discipline, and responding to emerging threats to the stability of the U.S. financial system. FSOC is chaired by the Secretary of the Treasury and its other voting members are the heads of CFPB, CFTC, FDIC, the Federal Reserve, Federal Housing Finance Agency, NCUA, OCC, SEC, and an insurance expert appointed by the President. Its nonvoting members are the directors of OFR and the Federal Insurance Office, and representatives from the state banking, securities, and insurance regulators.

FSOC's role in responding to systemic risks includes making nonbinding recommendations to federal agencies under Section 120 of the Dodd-

[27]The Currency and Foreign Transactions Reporting Act, its amendments, and other statutes relating to the subject matter of the act have come to be referred to as the Bank Secrecy Act. These statutes are codified as amended in scattered sections of Titles 12, 18, and 31 of the U.S. Code. Regulations implementing the Bank Secrecy Act primarily appear in 31 C.F.R. Ch. X. *See also* 31 C.F.R. § 1010.100(e).

[28]Oversight and enforcement of compliance with the BSA involve several federal agencies, including FinCEN and the Internal Revenue Service. FinCEN has delegated its BSA examination authority to other federal agencies, including the federal banking regulators, the Securities and Exchange Commission, the Commodity Futures Trading Commission, and the Federal Housing Finance Authority. *See* 31 C.F.R. § 1010.810(b); the federal banking regulators also have separate authority pursuant to 12 U.S.C. §§ 1786(q) and 1818(s) to ensure that banking organizations comply with BSA laws and regulations.

Frank Act.[29] FSOC also has three distinct designation authorities that, if invoked, generally require certain federal agencies to impose enhanced standards on designated entities or financial institutions conducting designated activities. These are the (1) nonbank designation authority, which allows FSOC to designate a nonbank financial company for supervision by the Federal Reserve and enhanced prudential standards; (2) financial market utility designation authority, which allows FSOC to designate a financial market utility as systemically important; and (3) payment, clearing, and settlement activities designation authority, which allows FSOC to designate a payment, clearing, or settlement activity as systemically important.[30]

Crypto Assets and Related Products Present Significant Risks and Challenges That Limit Potential Benefits

Starting with the development of Bitcoin in 2008, blockchain has underpinned the creation of crypto assets and associated trading platforms. Because of the characteristics of blockchain technology—especially the reduced need for intermediaries to make transactions—blockchain-related products and services have the potential to offer benefits over traditional financial products and services in some circumstances, including cost savings, faster transactions, and transparency. However, these benefits have not been fully realized. Furthermore, blockchain-related products and services present significant risks and challenges that have negative consequences for users and potentially the financial system, as evidenced by the turmoil in crypto markets in May and November 2022.

[29]The Dodd-Frank Act requires FSOC to report annually on recommendations to enhance U.S. financial stability, and FSOC has included such recommendations in each of its annual reports. Per Section 120 of the Dodd-Frank Act, FSOC may recommend that a primary financial regulator apply new or heightened standards for a financial activity or practice conducted by financial companies under the regulator's jurisdiction. If no primary regulator exists, FSOC can recommend appropriate legislation to Congress. Pub. L. No. 111-203, § 120, 124 Stat. 1376, 1408-1410 (2010) (codified at 12 U.S.C. § 5330).

[30]Financial market utilities are entities that manage or operate a multilateral system for the purpose of transferring, clearing, or settling payments, securities, or other financial transactions among financial institutions or between financial institutions and the entity, subject to certain exclusions. A payment, clearing, or settlement activity is carried out by one or more financial institutions to facilitate the completion of financial transactions, subject to certain limitations and exceptions.

Crypto Assets and Trading Platforms Could Provide Cheaper and Faster Transactions, but Pose Significant Volatility and Fraud Risks

Crypto assets take a variety of forms and are used to transfer value on blockchains.[31] Cryptocurrencies, an example of crypto assets, generally are digital representations of value protected through cryptographic mechanisms (instead of a central repository or authority), and typically are not government-issued legal tender.[32] Cryptocurrencies can fluctuate in value.

Stablecoins are a type of crypto asset designed with the intent to maintain a stable value, typically with reference to a fiat currency or other reference asset.[33] Stablecoins use different methods to try to maintain a stable value. Many stablecoins offer a promise or expectation that the coin can be redeemed at face value on request.

Crypto assets also include security tokens and crypto derivatives. Security tokens are issued on a blockchain and represent ownership or other rights. They are intended to be the digital forms of traditional securities such as stocks or bonds.[34] Crypto derivatives represent or function as derivatives. That is, they derive their value from an underlying crypto asset.[35]

Crypto asset platforms facilitate various types of crypto asset transactions and often serve as customers' entry point into the crypto asset

[31]Unless otherwise indicated, the terms we use to describe the examples of crypto assets are not defined in statute or regulation. Our list of crypto asset types is not exhaustive.

[32]GAO-22-104625.

[33]President's Working Group on Financial Markets, Federal Deposit Insurance Corporation, and the Office of the Comptroller of the Currency, *Report on Stablecoins* (Washington, D.C.: Nov. 1, 2021). Fiat currency is a national currency that derives its value from a country's promise to back it, not from physical commodities like gold or silver.

[34]The Securities Industry and Financial Markets Association defines securitized tokens as representations on distributed ledgers of securities issued on a nondistributed ledger platform. According to the association, such underlying securities should satisfy the definition of a security under applicable law. Securities Industry and Financial Markets Association and PricewaterhouseCoopers, LLP, *Security Tokens: Current Regulatory and Operational Considerations for Broker-Dealers and a Look Towards the Future* (New York City, N.Y.: Nov. 23, 2020). As with any security, security tokens offered to U.S. customers must be registered with SEC. Legal characterization of these assets are discussed later in this report.

[35]Global Blockchain Business Council, *Global Standards Mapping Initiative (GSMI) 2.0: Introduction to Crypto-Derivatives* (November 2021). Some common forms include crypto futures and options, many of which are structured similarly to traditional futures or options but have other crypto assets as the underlying asset.

ecosystem, according to some industry observers. For example, crypto asset trading platforms allow users to trade crypto assets for other crypto assets or fiat currency. These platforms may offer trading in a wide variety of cryptocurrencies and other crypto asset types, such as stablecoins. According to an industry observer, these platforms make it easier for users to transact in crypto assets than through peer-to-peer transactions, which users may find more complex and may require greater technological knowledge. Trading platforms may reduce the number of intermediaries by providing services that have been traditionally provided for by separate intermediaries, such as broker-dealer, custody, and clearing services.

A number of crypto asset platforms have been established to allow customers to lend and borrow cash and crypto assets. Crypto assets may be used as collateral for fiat or crypto asset loans—similar to a secured transaction in traditional finance. For example, a platform user could pledge a certain amount of Bitcoin and borrow Ethereum against it.[36] Some investors may use such platforms to earn interest on their crypto asset holdings by lending them out. They also may use the platform to borrow alternative crypto assets to engage in financial activities such as margin trading.[37] Other users may want to take out fiat loans secured by crypto assets instead of traditional assets.

The distributed nature of blockchain technology has the potential to provide benefits relating to the cost, speed, and transparency of transactions. For example, when transactions are publicly viewable, it offers greater transparency. In addition, reducing intermediaries could allow users to send and receive payments cheaper and faster than traditional financial services.[38] However, market conditions, features of the blockchain and of transaction verification, and other challenges may prevent potential benefits from being realized. More specifically,

- *Cost savings*. The use of blockchain has the potential to reduce costs for payments and other transactions by removing financial

[36]As of December 2022, Bitcoin and Ethereum were the two largest crypto assets in terms of market capitalization, according to Coinmarketcap.com.

[37]Margin trading refers to the practice of using borrowed funds from a broker to trade a financial asset, which forms the collateral for the loan from the broker.

[38]Benefits identified here are not necessarily comprehensive and may vary according to the type of crypto asset.

intermediaries that charge fees, such as for international transfers. According to the World Bank, as of March 2022, the global average remittance fee for traditional currency remittances was 6.09 percent per transfer, as compared to 2.02 percent for a cryptocurrency-based remittance, according to another study.[39] However, crypto asset companies and platforms generally charge users fees, which can increase in times of market stress.[40] Moreover, research indicates that the consensus protocol used on some blockchains consumes significantly more energy than traditional centralized databases, which can have global environmental effects.[41]

- *Faster transactions*. Some crypto asset transactions may be able to execute more quickly than traditional financial services. For example, some securities token transactions may be able to settle in less than a day. Traditional securities transactions currently settle 2 days after the transaction is executed. However, similar to fees rising during times of market stress, transaction times also can lengthen during abnormal market conditions.
- *Transparency*. Two industry observers told us certain crypto assets may provide greater transparency of some information than the traditional financial system. In permissionless (public) blockchains, any user, authority, or other observer can view raw transaction data, records, and history associated with a crypto asset transaction. However, such transparency also can be a drawback, because a user's privacy would be compromised if their crypto address were identified (anyone could view all their past transactions).

FDIC, OCC, Office of Domestic Finance, and SEC said that they had not seen evidence that the potential benefits of crypto assets had been

---

39The World Bank, "An Analysis of Trends in Cost of Remittance Services," *Remittance Prices Worldwide Quarterly*, issue 41 (March 2022). Also see Mercy Corps Ventures, *The potential of cryptocurrency for Kenya's youth: Pilot insights on stablecoin micropayments for digital workers* (Feb. 21, 2022).

40Fees are included to prevent spamming of transactions on a blockchain, and are used to reward those who verify transactions and add them to the blockchain (often called miners). They are also a mechanism to prioritize transactions, as miners prefer to include the most profitable transactions in a block. Fees generally spike when there is high network congestion, such as in times of market volatility. As of December 1, 2022, the highest recorded average transaction fee was $62.78 per transaction, recorded on April 21, 2021, according to bitinfocharts.com. The average transaction fee for Bitcoin was $1.75 per transaction, as of December 1, 2022.

41For a more detailed discussion of the energy consumption and environmental impact of blockchain, see GAO-22-104625.

realized. Additionally, the March 2023 Economic Report of the President stated that the vision of crypto assets creating a faster, cheaper, safer, and more inclusive U.S. payment system had not been realized and that crypto assets currently do not offer widespread economic benefits.[42]

Furthermore, crypto assets pose a number of significant risks, including those relating to volatility, market stability, intermediaries, fraud, and illicit activity.[43]

- *Volatility risk*. Prices of crypto assets typically have been highly volatile compared to other financial assets.[44] For example, according to Coinmarketcap.com, the value of one Bitcoin rose from about $960 in January 2017 to over $65,000 in November 2021. It then fell below $20,000 in June 2022 during the turmoil in the crypto asset markets precipitated by the collapse of a major stablecoin, TerraUSD. In November 2022, the collapse of FTX, the world's second-largest crypto asset trading platform, resulted in additional market turmoil that further reduced the value of many crypto assets. Because of their volatility, crypto assets may present greater risk than more traditional investments. This volatility hampers the ability of crypto assets to serve as an effective medium of exchange, according to some industry observers.

  Because crypto assets can be volatile, crypto asset lenders typically require borrowers to provide high levels of collateral to back their loans, according to industry observers. This introduces risks into crypto asset lending and borrowing. If the value of collateral drops, users may need to supply more collateral to secure the loan, making the loan more expensive for the borrower. Some platforms include terms that automatically liquidate collateral if the prices of the crypto assets used as collateral drop. This protects lenders from the risk of borrower default, but it presents a risk of loss for borrowers whose collateral would be liquidated.

---

[42]Executive Office of the President, Council of Economic Advisers, *Economic Report of the President* (Washington, D.C.: March 2023). The report is transmitted to Congress together with the *Annual Report of the Council of Economic Advisors*.

[43]Risks identified here are not comprehensive and vary according to the type of crypto asset.

[44]Yianni Doumenis, et al., "A Critical Analysis of Volatility Surprise in Bitcoin Cryptocurrency and Other Financial Assets," *Risks* 9, no. 11 (2021).

- *Market and financial stability risk*. Crypto assets are increasingly being integrated with traditional financial systems. For example, some investment funds invest in crypto assets and some retailers accept cryptocurrency as payment. According to an analysis by the International Monetary Fund, this integration increases the risk that the price volatility associated with these assets may spill over into traditional markets.[45] In March 2023, Silvergate Capital Corporation, the bank holding company for Silvergate Bank which had significant exposure to FTX deposits, announced the bank would be voluntarily liquidated following the withdrawal of almost 70 percent of its deposits. Similarly, in March 2023, Signature Bank, which had significant exposure to the digital asset industry, failed after large deposit withdrawals.[46] As discussed later, concerns exist that widespread use of stablecoins could pose risks to financial stability.
- *Intermediary risk*. Trading and lending platforms act as intermediaries by providing custody services or facilitating transactions and transfer of crypto assets. Some trading platforms have paused withdrawals and transactions during times of market stress, leaving many users unable to exit their positions. For example, during the turmoil in the crypto asset markets in May and June 2022, and more recently in November 2022, several prominent crypto asset trading platforms limited or froze customer withdrawals, resulting in financial harm to customers. Some of these platforms later filed for bankruptcy.

  The November 2022 FTX collapse revealed that the company had lent billions of dollars' worth of customer assets to its affiliated trading firm to fund risky investments. According to the firm's bankruptcy filing, the estimated number of creditors was more than 100,000. In a November 2022 statement, the FTX Chief Executive Officer, appointed to lead the company through bankruptcy, noted that a substantial portion of the platform's assets might be missing or stolen and that the firm lacked key internal controls, including controls to safeguard customer assets.

  Regulators also have raised concerns that reducing intermediaries and consolidating market functions into a crypto asset platform (such

[45]The author found that the volatility in Bitcoin prices explains 14–18 percent of the volatility in global equity prices. Tara Iyer, "Cryptic Connections: Spillovers between Crypto and Equity Markets," *Monetary and Capital Markets: Global Financial Stability Notes,* no. 2022/01 (Washington, D.C: International Monetary Fund, January 2022).

[46]See GAO, *Bank Regulation: Preliminary Review of Agency Actions Related to March 2023 Bank Failures*, GAO-23-106736 (Washington, D.C.: Apr. 28, 2023).

as taking custody of assets, settling trades, or clearing trades) may lead to conflicts of interest.[47] For instance, a platform that combines exchange and market making functions could have an incentive to trade ahead of its own customers, and could have less incentive to seek out best executions for its customers.

Some platforms may be susceptible to illicit trading practices, such as wash trading or front running, to manipulate crypto asset prices or to engage in self-dealing.[48] Aside from misconduct on a crypto asset trading platform, crypto asset markets are susceptible to manipulation of transactions on the part of validators who verify transactions and add them to the blockchain. Those validators can choose which transactions they add and in which order, and have incentives to prioritize the most profitable transactions. Therefore, a validator could place their order to buy or sell a crypto asset ahead of other pending transactions.

Some industry observers and state regulators have expressed concern that retail investors would bear the majority of the losses from bankruptcies of crypto asset trading platforms.[49] A number of uncertainties surround the treatment of custodially held customer assets in the event of a bankruptcy filing by a crypto asset entity.[50] Some industry observers have noted that if a bankruptcy court determines the assets are part of the crypto asset company's property—part of the bankruptcy "estate"—rather than customers' property, the court could determine that the customers are unsecured creditors who could lose some or all of the value of their assets. For example, in January 2023 a bankruptcy court determined that Celsius Network, a crypto asset lending platform that had filed for bankruptcy,

[47]Traditional securities and commodities markets consist of separate intermediaries, such as brokers, custodians, exchanges, market makers, transfer agents, and clearing agencies.

[48]Wash trading is the simultaneous or near-simultaneous purchase and sale of assets without an actual change in beneficial ownership, thereby artificially creating the appearance of trading volume in an asset. Front-running is the trading of a financial asset by someone who has knowledge of a future transaction to exploit the price movement from that transaction.

[49]At least 40 state securities regulators have opened an investigation into one crypto asset trading platform because of concerns relating to potential unregistered securities activity, mismanagement, securities fraud, and market manipulation. *In re* Celsius Network LLC, et al., Case No. 222-10964 (MG) (Bankr. S.D.N.Y. 2022).

[50]*See* Adam J. Levitin, *Not Your Keys, Not Your Coins, Unpriced Credit Risk in Cryptocurrency*, 101 Tex L. Rev. 877 (2023).

owned crypto assets that its customers had deposited into certain accounts on the platform. Based on the user agreements governing the accounts, the bankruptcy court found that the crypto assets became the property of Celsius when deposited and therefore property of the bankruptcy estate when Celsius filed for bankruptcy.[51] Factors that could affect an analysis of whether crypto assets held by a crypto asset platform become part of the bankruptcy estate include whether the property was held in trust by the crypto asset company and the terms of the account holders' agreements with the crypto asset companies.

- *Cybersecurity and theft risk*. Consumers and investors have experienced significant losses from fraud and scams involving crypto assets.[52] And as with any digital technology, digital crypto asset wallets may present cybersecurity risks. If wallets, or the platforms to which they are linked, are hacked, hackers can gain access to and steal users' crypto assets. If users lose funds due to wallet scams or hacks, it may be challenging for them to recover lost funds. One blockchain analytics firm reported that almost $10 billion worth of crypto assets were lost in 2022 due to theft or scams.[53]

  Furthermore, the purported tamper-resistant nature of blockchain has been called into question. One cybersecurity study noted that the integrity of the ledger could be compromised by subverting the properties of a blockchain's implementation, networking, and consensus protocol.[54] We also previously reported that advances in

---

[51] *In re* Celsius Network LLC, et al., 647 B.R. 631, 636-37 (Bankr. S.D.N.Y. 2023).

[52] In July 2017, SEC warned investors that fraudsters may entice investors by touting an initial coin offering as an investment opportunity, promising or guaranteeing high investment returns. Through an initial coin offering, a company that wishes to raise funds can issue fractionalized ownership of its company in a public offering through a crypto asset token instead of issuing traditional stock. SEC said it had taken multiple enforcement actions for fraud against these offerings. Securities and Exchange Commission, *Investor Bulletin: Initial Coin Offerings* (Washington, D.C.: July 25, 2017).

[53] Chainalysis, *The 2023 Crypto Crime Report* (February 2023).

[54] Evan Sultanik, et al., "Are Blockchains Decentralized? Unintended Centralities in Distributed Ledgers," *Trail of Bits* (New York: June 2022). Another study noted that no successful attacks have been launched on two important blockchains, Bitcoin and Ethereum. However, successful for-profit attacks have occurred against other blockchains in which supposedly immutable records have been maliciously rewritten. The study noted that changes to the blockchain protocol that erase previously accepted transactions can and do occur. See Francesca Carapella, et al., *Decentralized Finance (DeFi): Transformative Potential & Associated Risks*, Finance and Economics Discussion Series, 2022-057 (Washington, D.C.: August 2022).

quantum computing may generate longer-term risks to the security of encrypted data stored on blockchains.[55]

- *Information asymmetry risk*. Crypto asset issuers and platforms may not fully disclose material information about an investment or a platform, including risks undertaken by consumers and investors or conflicts of interest. For example, lenders seeking high yields may supply crypto assets to a lending platform without full information about risks taken by the platform and the potential for significant losses. In a February 2022 enforcement action, SEC found that a prominent lending platform made a false and misleading statement on its website for more than 2 years concerning the level of risk in its loan portfolio and lending activity.[56]
- *Illicit activity risk*. Law enforcement officials previously told us that the perception of anonymity makes crypto asset a preferred tool for certain types of trafficking and money-laundering activities.[57] Some trading platforms were found to conduct illicit finance activities, including money laundering and sanctions evasion. For example, in October 2022, FinCEN fined the owner of a crypto assets trading platform $29 million for violations of the BSA and FinCEN's implementing regulations. FinCEN found the platform conducted transactions involving high-risk jurisdictions subject to U.S. sanctions, and failed to file suspicious activity reports on significant numbers of transactions.[58] Terrorists also have been using crypto asset trading platforms, and we previously reported that crypto assets pose an emerging terrorist finance vulnerability because they are accessible

[55]See GAO-22-104625; and *Quantum Computing and Communications: Status and Prospects*, GAO-22-104422 (Washington, D.C.: Oct. 19, 2021). Federal agencies and academic researchers are involved in research and development of post-quantum cryptography systems designed to be secure against decryption attempts using either quantum or classical computers. The National Institute of Standards and Technology has been developing standards to support deployment of new post-quantum cryptography infrastructure.

[56]BlockFi Lending LLC, Securities Act Rel. No. 11029, Investment Company Act Rel. No. 34503, SEC File No. 3-20758, 2022 WL 462445 (Feb. 14, 2022). SEC alleged that BlockFi Lending LLC failed to register the offers and sales of its retail crypto lending product and that it allegedly operated as an unregistered investment company in violation of the Investment Company Act of 1940.

[57]GAO, *Trafficking and Money Laundering: Strategies Used by Criminal Groups and Terrorists and Federal Efforts to Combat Them*, GAO-22-104807 (Washington, D.C.: Dec. 23, 2021).

[58]Bittrex, Inc., FinCEN No. 2022-03 (2022). FinCEN's action was part of a global settlement with Treasury's Office of Foreign Assets Control.

from anywhere and often difficult to trace.[59] However, we found that it can be easier for law enforcement to track crypto asset activities than cash-based transactions, which leave no digital trail. For example, public blockchains allow investigators to trace transactions and participants.

Openness of Decentralized Finance Products and Services Offers Potential Benefits and Poses Risks

Blockchain-related financial products and services exist on a spectrum of decentralization. Some blockchain-related financial products and services have centralized operators or administrators, such as companies that operate platforms to provide products and services to users. Centralized crypto asset trading platforms typically take custody of users' crypto assets and may provide services such as order book management and matching.[60]

In contrast, products and services referred to as decentralized finance, or DeFi, operate on peer-to-peer networks running on blockchain platforms. According to the International Organization of Securities Commissions, DeFi refers to the use of blockchain to eliminate the need for some traditional financial intermediaries and centralized institutions in the provision of financial products and services.[61] Underlying protocols and smart contracts are typically used to deliver DeFi products and services to users. DeFi participants can view the underlying source code and build their own product. Furthermore, individual DeFi products and services can be combined to create new products and services. DeFi products and services are also generally noncustodial, where users self-custody their crypto assets.

Governance within DeFi products and services refers to the ways in which collective decisions are made and changes to protocols are implemented. DeFi products and services fall along a governance spectrum ranging from centralized, where the operator controls protocol decisions and changes directly, to decentralized, where governance

[59]GAO, *Financial Technology: Additional Steps by Regulators Could Better Protect Consumers and Aid Regulatory Oversight*, GAO-18-254 (Washington, D.C.: Mar. 22, 2018).

[60]Order book refers to an electronic list of buy and sell orders for a specific financial instrument organized by price level. Matching orders is the process by which a platform pairs one or more unsolicited buy orders to one or more sell orders to make trades.

[61]International Organization of Securities Commissions, *IOSCO Decentralized Finance Report*, OR 01/2022 (Madrid, Spain: March 2022).

token holders make decisions and any changes to DeFi protocols.[62] DeFi products and services may move from centralized governance at their outset to fully decentralized governance as they reach maturity. However, many products and services described as DeFi today remain somewhat centralized, according to regulators. For example, DeFi products and services that are still operated, controlled, or influenced by their initial developers could be considered centralized by regulators.

By removing intermediaries, DeFi has the potential to allow for faster, cheaper, and more efficient execution of transactions. DeFi products and services are generally openly accessible, and users with the necessary skills can use the underlying code to develop new products and services. According to some industry participants, this may benefit users and markets by enabling the development of more complex or comprehensive financial services through DeFi protocols. The openness of DeFi protocols could also enhance their transparency. For example, any user could look at underlying code to understand how it works and what features or terms are built into it. The noncustodial design of many DeFi products and services also may benefit users by allowing them to maintain full control of their own assets, which could help them avoid some of the intermediary risks described above.

However, DeFi may result in increased risks compared to centralized blockchain products and services or traditional finance. The removal of intermediaries has raised questions from regulators about who is responsible for ensuring compliance with law and regulation, such as those intended to protect consumers and investors and counter illicit finance. Users of DeFi products and services also take upon themselves risks that a traditional financial intermediary or a centralized crypto asset product or service provider otherwise assumes. For example, because DeFi products and services are noncustodial, users are responsible for the security of their own assets, just as with noncustodial wallets.

Risk of loss is generally present in financial services, but without central entities involved in DeFi products and services, users who lose funds may have little to no recourse. Additionally, industry observers noted the open-source and transparency features of DeFi products and services may allow malicious actors to exploit DeFi protocol code for gain. Furthermore, any coding errors in a DeFi protocol or underlying smart contract could

[62]Governance tokens may give holders voting rights on certain future aspects of a specific blockchain protocol. Holders of governance tokens may be able to propose and vote on certain changes to smart contracts or other blockchain protocols.

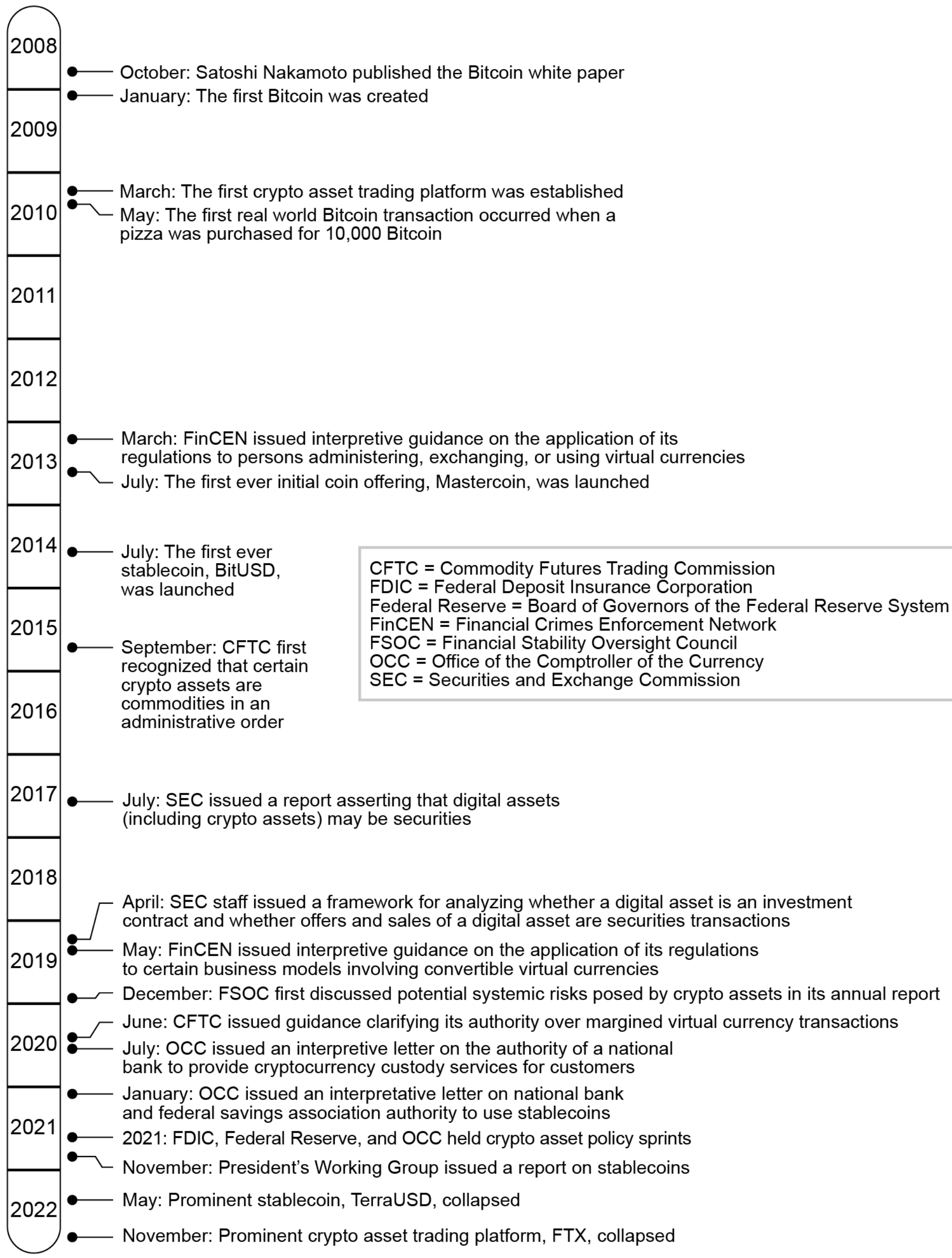
lead to financial loss for users if the errors cause the protocol or smart contract to fail to execute as expected. Depending on a DeFi product or service's governance structure, it could be difficult to make changes to fix such an issue. Also, because blockchain-related products and services often aim to remove intermediaries, there also may be legal uncertainty around who is responsible if there is a mistake on the blockchain.

Regulatory Jurisdiction for Crypto Assets Varies Based on the Intermediary and Activity

Financial Regulators Have Taken or Planned Steps to Clarify Crypto Asset Jurisdiction

Federal financial regulators—SEC, CFTC, FinCEN, federal banking regulators, and CFPB—oversee regulated institutions' engagement with crypto assets. In recent years, these regulators have provided some guidance or taken other actions intended to clarify their jurisdiction and regulatory requirements for crypto asset-related activities of financial intermediaries. See figure 2 below for selected crypto-related regulatory actions.

Figure 2: Selected Crypto-related Regulatory Actions and Market Events, 2008–2022



Source: GAO. | GAO-23-105346

Securities and Exchange Commission

Determining whether an asset is a security under federal securities laws depends on facts and circumstances, as previously discussed. SEC has determined certain crypto assets to be securities under federal securities laws and subject to SEC oversight, including registration and disclosure requirements. In July 2017, SEC issued an investigative report asserting that digital assets (including crypto assets) may be securities and therefore subject to the agency's jurisdiction.[63] In April 2019, SEC staff issued a framework for analyzing whether a digital asset is an investment contract and whether offers and sales of a digital asset are securities transactions (see text box).[64]

[63]Securities and Exchange Commission, Exchange Act Rel. No. 81207, Report of Investigation Pursuant to Section 21(a) of the Securities Exchange Act of 1934: The DAO (July 25, 2017). In this report, SEC determined that the unregistered 2016 offering of tokens by a group known as "The DAO," a decentralized autonomous organization, were investment contracts and therefore were securities for purposes of the securities laws and subject to regulation. SEC chose not to pursue legal action or enforcement. Instead, SEC issued the report (The DAO Report) cautioning the industry and market participants that offers and sales of digital assets by "virtual" organizations are subject to the requirements of the federal securities laws. The report said that determining whether a particular investment transaction involves the offer or sale of a security will depend on the facts and circumstances, including the economic realities of the transaction.

[64]Securities and Exchange Commission, *Framework for "Investment Contract" Analysis of Digital Assets* (Washington, D.C.: Apr. 3, 2019). This framework represents the views of staff from SEC's Strategic Hub for Innovation and Financial Technology and the Commission neither approved nor disapproved its content.

SEC Investment Contract Analysis Framework

In April 2019, SEC staff issued a framework for analyzing whether a digital asset is an investment contract and whether offers and sales of a digital asset are securities transactions. According to this framework, the offer and sale of digital assets typically involves the investment of money in a common enterprise under the *Howey* test. Determining whether the purchaser has a reasonable expectation of profits derived from the efforts of others generally requires further analysis. That part of the *Howey* test is met when a promoter, sponsor, or other third party ("active participant") provides essential managerial efforts that affect the success of the enterprise and investors reasonably expect to derive profit from those efforts.

The framework identifies several factors to assist in applying the *Howey* test and subsequent case law. The framework explains that the following inquiries are relevant to an analysis of whether the "efforts of others" part of the *Howey* test is satisfied: (1) whether the purchaser reasonably expects to rely on the efforts of the promotor or sponsor and whether those efforts are significant; (2) whether there is a reasonable expectation of profits; and (3) the economic reality of the transaction, which can include consideration of whether the instrument is offered or sold for use or consumption by purchasers. The framework outlines characteristics relevant to each of the inquiries. For example, in determining whether the purchaser of a digital asset relies on the efforts of others, the purchaser can consider whether the sponsor or promoter (1) is responsible for the development, improvement, operation, or promotion of the network; (2) creates or supports a market for or the price of, the digital asset; (3) has a lead or central role in the direction of the ongoing development of the network or the digital asset; and (4) has a continuing managerial role in making decisions about the network or rights to the digital asset. The framework notes that listed characteristics are not intended to be exhaustive in evaluating whether a digital asset is an investment contract and that no single factor is determinative.

Source: Securities and Exchange Commission (SEC). | GAO-23-105346

The securities laws require registration of the offers and sales of crypto assets that are securities, as well as registration of market participants involved in crypto asset securities (crypto assets that meet the definition of securities under federal securities laws), including broker-dealers, investment funds and advisers, and securities exchanges. Therefore, blockchain-related product and service providers that transact in crypto asset securities must register as appropriate. For example, a crypto asset trading platform offering trading in crypto asset security tokens and operating as an exchange as defined by federal securities laws is expected to register with SEC as a national securities exchange, or qualify for an exemption.[65]

SEC and its staff have issued some guidance to crypto asset market participants intended to clarify regulatory requirements. For example, market participants have raised questions concerning the application of SEC's custody requirements for broker-dealers facilitating customers' transactions in crypto asset securities. In 2019, staffs of FINRA and SEC issued a Joint Statement on broker-dealer custody of crypto asset securities that described models for registered broker-dealers activities involving such securities. These models do not involve the broker-dealer engaging in custody functions.[66]

In September 2020, SEC staff issued a no-action letter to FINRA supplementing the Joint Statement for registered broker-dealers that operate alternative trading systems. The no-action letter described another model for alternative trading systems to facilitate transactions in crypto asset securities involving third-party custodians where the broker-dealer does not exercise any level of control over the customers' assets other than by notifying the custodians of the transactions. If the broker-dealer operating an alternative trading system uses the model and meets certain conditions described in the no-action letter, SEC staff will not

[65]Any organization, association, or group of persons, whether incorporated or unincorporated, that constitutes, maintains, or provides a market place or facilities for bringing together purchasers and sellers of securities must register with SEC as a national securities exchange or obtain an appropriate exemption. 15 U.S.C. §§ 78c(a)(1), 78f. SEC regulations at 17 C.F.R. § 240.3b-16(a) further define "exchange." An organization, association, or group of persons that meets the criteria of Rule 3b-16(a) is exempt from the statutory definition of "exchange" if it instead registers with the SEC as a broker-dealer and complies with Regulation ATS.

[66]Securities and Exchange Commission Division of Trading and Markets and Financial Industry Regulatory Authority Office of General Counsel, *Joint Staff Statement on Broker-Dealer Custody of Digital Asset Securities* (July 8, 2019). Broker-dealers must comply with the custodial requirement of Rule 15c3-3 under the Securities Exchange Act of 1934. The rule requires broker-dealers to obtain and maintain physical possession or control of all fully-paid and excess margin securities they carry for the account of customers. 17 C.F.R. § 240.15c3-3(b). The non-custodial models discussed in the statement would not raise the same compliance concern for the staff as long as broker-dealers comply with other laws and regulations. The Joint Staff Statement discussed the challenge of complying with the provision due to the nature of crypto asset securities.

recommend enforcement action to the Commission.[67] In December 2020, SEC issued a statement and request for comment regarding broker-dealer custody of crypto asset securities. The statement provides that SEC will not take certain enforcement actions against a broker-dealer that maintains custody of crypto asset securities for a period of 5 years. The broker-dealer must limit its business to activities involving crypto asset securities and comply with certain other conditions.[68]

Commodity Futures Trading Commission

CFTC has determined that certain crypto assets such as Bitcoin, Ethereum, and certain stablecoins are commodities under the Commodity Exchange Act.[69] CFTC regulates derivatives exchanges that trade crypto asset commodity derivatives (such as futures contracts on Bitcoin) and requires registration from and regulates market participants that transact with such derivatives. For example, a crypto asset trading platform that provides trading in these derivatives is expected to register as a

---

[67]Securities and Exchange Commission Division of Trading and Markets, Letter to Ms. Kris Dailey, Financial Industry Regulatory Authority, *ATS Role in the Settlement of Digital Asset Security Trades* (Washington, D.C.: Sept. 25, 2020). The no-action letter indicated that a broker-dealer could operate an alternative trading system using either of two models for facilitating secondary transactions in crypto asset securities: a four-step process described in the 2019 Joint Statement or a three-step process. The no-action letter stated that broker-dealers seeking to operate an alternative trading system assert that the primary benefit of the three-step settlement process is that it would reduce operational and settlement risk. SEC staff have issued several no-action letters in connection with firms conducting activities related to crypto asset securities, in which agency staff state that they do not intend to recommend an enforcement action against a firm if it offers products or operates in the way described by the firm in a no-action request letter to the regulator. SEC staff said the no-action letter process allows for engagement with companies and offers insight into their products and services, while potentially providing a degree of comfort to the participating companies.

[68]*Custody of Digital Asset Securities by Special Purpose Broker-Dealers,* 86 Fed. Reg. 11627 (Feb. 26, 2021). The statement sets forth SEC's position that for a period of 5 years, a broker-dealer operating under the circumstances set forth in the statement will not be subject to an enforcement action on the basis that the broker-dealer deems itself to have obtained and maintained physical possession or control of customer fully paid and excess margin digital asset securities for the purposes of paragraph (b)(1) of Rule 15c3-3. These circumstances include that the broker-dealer limits its business to digital asset securities, establishes and enforces policies and procedures reasonably designed to mitigate the risks associated with conducting a business in digital asset securities, and provides customers with certain written disclosures regarding the risks of engaging in transactions involving digital asset securities.

[69]CFTC staff stated that it is now widely accepted by agencies, courts, and market participants that certain crypto assets are commodities as the Commodity Exchange Act defines that term. CFTC first determined that certain crypto assets are commodities within the meaning of the CEA in the administrative order Coinflip, Inc., d/b/a/ Derivabit and Francisco Riordan, CFTC No. 15-29, 2015 WL 5535736 (Sept. 17, 2015).

designated contract market with CFTC (unless another regulatory category applies).

While CFTC has limited authority to directly regulate spot market transactions, the Commodity Exchange Act grants CFTC authority to enforce certain provisions of the act in connection with certain commodity transactions entered into with, or offered to (even if not entered into with) a retail customer on a leveraged, margined or financed basis as if the transactions were futures contracts.[70] In June 2020, CFTC issued final interpretive guidance clarifying that leveraged, margined, or financed transactions in virtual currency offered to retail customers are subject to CFTC oversight and the transactions must be conducted on or subject to the rules of designated contract markets, absent an exception.[71]

FinCEN

In interpretive guidance issued in March 2013, FinCEN determined that BSA/AML regulations applicable to money transmitters apply to virtual currency exchangers and administrators—such as crypto asset platforms that exchange virtual currencies and stablecoin administrators that

[70] 7 U.S.C. § 2(c)(2)(D). The Commodity Exchange Act provides certain exceptions from this treatment, including for contracts of sale that result in "actual delivery" within 28 days from the trade date. 7 U.S.C. § 2(c)(2)(D)(ii)(III)(aa).

[71] In the June 2020 guidance, CFTC interpreted "virtual currency" to encompass any digital representation of value that functions as a medium of exchange, and any other digital unit of account that is used as a form of a currency (transferred from one party to another as a medium of exchange); may be manifested through units, tokens, or coins, among other things; and may be distributed by way of smart contracts, among other structures. In issuing the guidance, CFTC stated that the definition was used to delineate the scope of the interpretation of "actual delivery" in 7 U.S.C. § 2(c)(2)(D). CFTC has noted that it did not intend to create a bright-line definition given the evolving nature of the commodity and, in some instances, the underlying public distributed ledger technology. 85 Fed. Reg. 37734 (June 24, 2020).

conduct transactions in stablecoin.[72] FinCEN defined virtual currency as a medium of exchange that can operate like currency in some environments but does not have all the attributes of "real" currency, including legal tender status. FinCEN applies its regulations to "convertible virtual currency," which has an equivalent value in real currency or acts as a substitute for real currency.[73] FinCEN subsequently issued additional interpretative guidance in May 2019 reiterating its earlier guidance and providing further clarification on the application of BSA/AML regulation to other common business models involving convertible virtual currencies.[74]

Federal Banking Regulators

Federal banking regulators supervise their institutions' blockchain-related activities, including their engagement with crypto assets. Staff from all four federal banking regulators told us that while banks may be permitted to engage in certain crypto-related activities, depending on the activity, a limited number have chosen to do so. They said that examples of the types of services these banks may provide include custody services for customers' crypto assets (often through a third-party service), holding

[72]A money transmitter includes a person—such as an individual, corporation, or partnership—that provides money transmission services. FinCEN defines money transmission as "the acceptance of currency, funds, or other value that substitutes for currency from one person and the transmission of currency, funds, or other value that substitutes for currency to another location or another person by any means." Whether a person is a money transmitter for BSA purposes is a matter of facts and circumstances. 31 C.F.R. § 1010.100(ff)(5). Under FinCEN's BSA/AML regulations, money transmitters are a type of money services business. FinCEN defines a virtual currency exchanger as a person engaged as a business in the exchange of virtual currency for real currency, funds, or other virtual currency. It defines a virtual currency administrator as a person engaged as a business in issuing (putting into circulation) a virtual currency, and who has the authority to redeem (to withdraw from circulation) such virtual currency. See Financial Crimes Enforcement Network, *Application of FinCEN's Regulations to Persons Administering, Exchanging, or Using Virtual Currencies* (Washington, D.C.: Mar. 18, 2013).

[73]The interpretative guidance clarifies that an administrator or exchanger that (1) accepts and transmits a convertible virtual currency or (2) buys or sells convertible virtual currency for any reason is a money transmitter under FinCEN's regulation.

[74]See Financial Crimes Enforcement Network, *Application of FinCEN's Regulations to Certain Business Models Involving Convertible Virtual Currencies* (Washington, D.C.: May 19, 2019).

stablecoins' reserves, or providing deposit services for crypto asset market participants.[75]

Federal banking regulators have issued guidance to their supervised institutions regarding the legal permissibility of crypto asset-related activities. For example, OCC issued interpretive letters clarifying that national banks and federal savings associations can offer safekeeping and other custody services for cryptographic keys associated with crypto assets and addressing their authority to issue stablecoins for facilitating payments.[76] In January 2021, OCC also issued an interpretive letter on the authority of OCC to charter national trust banks and concluded that national trust banks have the authority to perform fiduciary and nonfiduciary activities, including certain activities permissible under state law for a state trust bank.[77] As of August 2022, two state-chartered trust companies engaged in crypto asset-related activities received conditional approval from OCC to convert their state charters to uninsured national trust bank charters and OCC granted preliminary conditional approval of

[75]Custody services typically include the settlement, safekeeping, and reporting of customers' assets, such as marketable securities and cash.

[76]Office of the Comptroller of the Currency, *Authority of a National Bank to Provide Cryptocurrency Custody Services for Customers*, Interpretive Letter #1170 (Washington, D.C.: July 22, 2020); and *OCC Chief Counsel's Interpretation on National Bank and Federal Savings Association Authority to Use Independent Node Verification Networks and Stablecoins for Payment Activities*, Interpretive Letter #1174 (Washington, D.C.: Jan. 4, 2021).

[77]Office of the Comptroller of the Currency, *OCC Chief Counsel's Interpretation on National Trust Banks*, Interpretive Letter #1176 (Washington, D.C.: Jan. 11, 2021). The interpretive letter noted that 12 U.S.C. § 27(a) recognizes that OCC has the authority to charter a national bank that limits its activities to those of a trust company and related activities. Activities of a trust company include activities permissible for a state bank or trust company, even if those activities are not necessarily considered fiduciary under 12 U.S.C. § 92a and OCC regulations. Typically, trust bank activities focus on holding assets on behalf of customers, acting as trustees or other fiduciaries, and executing transactions on behalf of customers or at their direction. OCC has issued guidance on capital and liquidity specific to national trust banks. Office of the Comptroller of the Currency, *Supervision of National Trust Banks: Revised Guidance: Capital and Liquidity,* OCC Bulletin 2007-21 (Washington, D.C.: June 26, 2007).

an application to charter an uninsured, de novo national trust bank.[78] Examples of services these entities proposed providing included crypto asset custodying, lending, and platform services. However, one of the conditional approvals and the preliminary conditional approval subsequently expired.[79]

OCC, the Federal Reserve, and FDIC require the institutions they supervise to notify them before engaging in crypto-related activities. In November 2021, OCC published an interpretive letter clarifying that the activities addressed in its prior interpretive letters are legally permissible provided a bank can demonstrate to the satisfaction of its supervisory office that it can conduct the activities in a safe and sound manner.[80] The letter outlined a process for requesting and obtaining written supervisory non-objection from OCC before conducting new crypto asset activities under the prior letters. The Federal Reserve issued a supervisory letter in August 2022 requiring its supervised institutions to verify any crypto asset-related activity is legally permissible and notify the Federal Reserve about the activity before they engage in it.[81] Similarly, in April 2022, FDIC issued a financial institution letter requiring supervised institutions that are currently engaged in or intend to engage in crypto asset-related activities to notify FDIC. FDIC stated it would review the information and provide relevant supervisory feedback.[82]

---

[78]Office of the Comptroller of the Currency, *Re: Application by Anchorage Trust Company, Sioux Falls, South Dakota to Convert to a National Trust Bank*, OCC Control Number: 2020-WE-Conversion-317667 (Jan. 13, 2021); *Re: Application by Protego Trust Company, Seattle, Washington, to Convert to a National Trust Bank*, OCC Control Number: 2020-HQ-Conversion-318271 (Feb. 4, 2021); and *Re: Application to Charter Paxos National Trust, New York, New York*, OCC Control Number: 2020-NE-Charter-318305 (Apr. 23, 2021).

[79]Protego Trust Bank's conditional approval expired in February 2023. Similarly, Paxos National Trust's preliminary conditional approval expired in March 2023.

[80]Office of the Comptroller of the Currency, *Chief Counsel's Interpretation Clarifying: (1) Authority of a Bank to Engage in Certain Cryptocurrency Activities; and (2) Authority of the OCC to Charter a National Trust Bank*, Interpretive Letter #1179 (Washington, D.C.: Nov. 18, 2021).

[81]Board of Governors of the Federal Reserve System, *Engagement in Crypto-Asset-Related Activities by Federal Reserve-Supervised Banking Organizations*, SR 22-6 (Washington, D.C.: Aug. 16, 2022).

[82]Federal Deposit Insurance Corporation, *Notification of Engaging in Crypto-Related Activities*, FIL-16-2022 (Washington, D.C.: Apr. 7, 2022).

NCUA does not require similar notification. But, in a May 2022 letter to credit unions, NCUA stated that when considering a blockchain-related platform, product, or service, credit unions should first evaluate the permissibility of the activity itself and then assess the opportunities and risks relative to the activity and the underlying technology.[83]

In 2021, FDIC, the Federal Reserve, and OCC conducted a series of interagency policy "sprints" focused on crypto assets. Specifically, agency staff conducted preliminary analysis on developing a taxonomy of crypto assets, identifying key risks, assessing the applicability of existing regulations and guidance, and identifying areas that may benefit from additional clarification. The areas they identified where greater clarity was needed included legal permissibility of certain activities related to crypto assets conducted by banks and expectations for safety and soundness, consumer protection, and compliance with existing laws and regulations related to custody services. As of September 2022, agency staff said they were working on these policy clarifications but had not yet determined a date for releasing published guidance.

Federal banking regulators issued several statements in response to the significant volatility and the exposure of vulnerabilities in the crypto asset sector in recent months.

- In January 2023, FDIC, the Federal Reserve and OCC issued a joint statement highlighting key risks to banking organizations associated with crypto assets and participants in the crypto asset sector.[84] These included the risks of fraud and scams among sector participants; significant volatility in crypto asset markets, the effects of which include potential impacts on deposit flows associated with crypto asset companies; and risk within the sector resulting from interconnections among certain participants, including through opaque lending and investing arrangements. It noted that such interconnections also may present concentration risks for banking organizations with exposures to the crypto asset sector.

[83]National Credit Union Administration, *Federally Insured Credit Union Use of Distributed Ledger Technologies,* 22-CU-07 (Washington, D.C.: May. 25, 2022).

[84]Office of the Comptroller of the Currency, Board of Governors of the Federal Reserve System, and Federal Deposit Insurance Corporation, *Joint Statement on Crypto-Asset Risks to Banking Organizations* (Washington, D.C.: Jan. 3, 2023).

- In January 2023, the Federal Reserve issued a policy statement on its general belief that the same bank activity, presenting the same risks, should be subject to the same regulatory framework regardless of which agency supervises the bank.[85] The policy statement provides that the Federal Reserve has authority to generally prohibit state member banks and their subsidiaries from engaging as principal in any activity—including crypto asset activity—that is not permissible for a national bank unless authorized under federal statute or under FDIC regulations. If an activity is permitted for national banks by OCC, a state member bank may engage in the activity subject to the same terms, conditions, and limitations placed on national banks by OCC. The policy statement applies to insured and uninsured state member banks and is intended to mitigate the risks of regulatory arbitrage among banks with different charters and federal supervisors.[86]
- In February 2023, FDIC, the Federal Reserve, and OCC issued a joint statement on the liquidity risks presented by certain sources of funding from crypto asset-related entities, and some effective practices to manage such risks.[87]

Consumer Financial Protection Bureau

CFPB staff told us they have been evaluating the full scope and applicability of CFPB's current authorities for crypto assets. They noted that at least some products or services offered to consumers may qualify as consumer financial products or services under CFPB's jurisdiction. These may include credit, debit, and prepaid cards that offer rewards in crypto assets, direct deposit arrangements onto crypto asset accounts, and the storage and use of consumers' U.S. dollars in accounts held by consumers on crypto asset platforms. In December 2021, CFPB initiated an investigation into a firm offering a crypto asset lending product to

[85]Board of Governors of the Federal Reserve System, *Policy Statement on Section 9(13) of the Federal Reserve Act* (Washington, D.C.: Jan. 27, 2023). The Federal Reserve has discretion under section 9(13) of the Federal Reserve Act to limit the activities of a state member bank and its subsidiaries to those activities that are permissible for a national bank in a manner consistent with section 24 of the Federal Deposit Insurance Act. 12 U.S.C. § 330. Section 24 of the Federal Deposit Insurance Act generally prohibits insured state banks from engaging as principal in any activity that is not permissible for national banks, unless authorized by federal statute or FDIC. 12 U.S.C. § 1831a(a); 12 C.F.R. part 362.

[86]Regulatory arbitrage occurs when institutions take advantage of variations in how agencies implement regulatory responsibilities in order to be subject to less scrutiny.

[87]Office of the Comptroller of the Currency, Board of Governors of the Federal Reserve System, and Federal Deposit Insurance Corporation, *Joint Statement on Liquidity Risks to Banking Organizations Resulting from Crypto-Asset Market Vulnerabilities* (Washington, D.C.: Feb. 23, 2023).

determine, in part, whether it was engaged in conduct that is subject to federal consumer financial law.[88]

Many Crypto Firms Are Not Registered with SEC and CFTC, According to Agency Officials

SEC officials said that many crypto assets are likely securities and many crypto asset platforms trade these securities without registering as a national securities exchange. They noted that risks to investors increase when securities tokens and their trading platforms are unregistered and not subject to appropriate oversight. As of December 2022, no trading platforms were registered as national securities exchanges according to SEC staff. The SEC Chair has called for unregistered firms transacting in crypto asset securities to register with SEC.

Similarly, CFTC officials said trading platforms that offer crypto commodity derivatives without registering as designated contract markets increase risks to consumers. As of December 2022, five platforms were registered as designated contract markets, according to CFTC staff. A September 2022 Treasury report stated that the risks associated with crypto asset trading platforms that are not in compliance with U.S. laws and regulations, or that may not be regulated, are significant.[89] It stated that such risks arise from a lack of compliance with disclosure requirements for registered exchanges and products that are designed to provide investors and customers with material and relevant information and market conduct requirements designed to provide fair, orderly, and efficient markets.

As previously discussed, SEC and CFTC and their staff have issued some guidance to the industry intended to clarify jurisdiction and facilitate regulatory compliance. Both agencies also took enforcement actions that address lack of compliance with registration requirements. As of December 2022, SEC had taken over 100 enforcement actions related to crypto assets—including those against crypto asset trading platforms functioning as unregistered national securities exchanges. In May 2022, SEC announced it increased its Crypto Assets and Cyber Unit (in the Division of Enforcement) from 30 staff to 50 staff to address fraudulent,

[88]CFPB disclosed the investigation in November 2022 when the CFPB director issued a decision and order denying the firm's petition to CFPB to set aside or modify the agency's civil investigative demand. Nexo Financial LLC, 2022-MISC-Nexo Financial LLC-0001 (Nov. 22, 2022).

[89]Department of the Treasury, *Crypto-Assets: Implications for Consumers, Investors, and Businesses* (Washington, D.C.: Sept. 16, 2022).

unregistered, and other unlawful crypto asset activities.[90] As of December 2022, CFTC brought over 60 enforcement actions related to crypto assets, including actions alleging that crypto asset trading platforms functioned as unregistered designated contract markets, swap execution facilities, and futures commission merchants, as well as actions alleging fraud and manipulation in connection with crypto assets.

Some crypto market participants have raised questions about the regulatory status of some crypto assets in which they transact and called for additional clarity from regulators. For example, some market participants and observers have stated they have difficulty applying the SEC staff's 2017 framework for determining whether a given crypto asset constitutes an investment contract and thus a security under the federal securities laws.[91] Additionally, some companies subject to an ongoing SEC enforcement action challenged SEC's findings that the crypto assets in which they transact are securities under federal securities laws.[92]

Some crypto-industry market participants and observers have also raised questions about how to register and comply with regulatory requirements. They noted that unlike traditional securities exchanges, crypto asset

[90]Securities and Exchange Commission, *SEC Nearly Doubles Size of Enforcement's Crypto Assets and Cyber Unit*, Press Release 2022-78 (Washington, D.C.: May 3, 2022).

[91]One market observer stated in recent Congressional testimony that SEC staff's guidance for determining whether a digital asset is a security does not provide certainty for this analysis, because it provides a non-exclusive list of characteristics to be considered when analyzing how likely a digital asset is to be a security. See House Committee on Financial Services, Subcommittee on Digital Assets, Financial Technology, and Inclusion, *The Future of Digital Assets: Identifying the Regulatory Gaps in Digital Asset Market Structure*, 118th Cong. (Apr. 27, 2023); statement of Zachary J. Zweihorn, Partner, Davis Polk & Wardwell LLP.

[92]*See SEC v. Ripple Labs Inc. et al.,* No. 20-cv-10832 (S.D.N.Y. filed Dec. 22, 2020). SEC alleged that Ripple Labs, Inc. and two executives violated securities laws by selling a crypto asset security, the XRP digital coin, without registration. SEC has been generally successful in court cases decided to date brought against issuers for unregistered securities offerings. *See SEC v. LBRY, Inc.,* No. 21-cv-260-PB, 2022 WL 16744741 (D.N.H. Nov. 7, 2022) (determining on a motion for summary judgment that the crypto assets that LBRY offered and sold were unregistered securities in violation of Section 5 of the Securities Act of 1933); *SEC v. Telegram Grp. Inc.*, 448 F. Supp. 3d 352 (S.D.N.Y. 2020) (granting preliminary injunction on finding that SEC has shown a substantial likelihood of success in proving that the plan to distribute assets would be an unregistered offering of securities); and *SEC v. Kik Interactive Inc*., 492 F. Supp. 3d 169 (S.D.N,Y.2020) (granting SEC motion for summary judgment finding that Kik's digital token offering was the offer and sale of securities without a registration statement that violated Section 5 of the Securities Act of 1933).

trading platforms may trade both security and nonsecurity assets and provide other services that separate intermediaries—such as broker-dealer, custody, and clearing services—traditionally provided.[93]

One crypto asset firm provided recent Congressional testimony stating that existing national securities exchange regulation does not address whether nonsecurities can trade alongside securities on crypto asset trading platforms and is not designed to accommodate direct investor access to trading without the use of intermediaries.[94] For example, it noted that existing national securities exchange requirements do not allow for disintermediated trading because national securities exchanges require members to trade directly and such membership is available only to broker-dealers.[95]

In a September 2022 speech, the SEC Chair stated his view that most crypto assets are securities because they are investment contracts under the *Howey* test.[96] He noted that some crypto asset market participants called for further guidance from SEC, but stated that SEC has provided guidance through, among other things, the 2017 DAO report, enforcement actions, and the 2019 SEC staff framework for investment contract analysis.

With respect to crypto asset intermediaries, the SEC chair stated he asked SEC staff to consider how investors might be allowed to trade

[93]An SEC commissioner stated that these questions needed to be answered if these platforms determine to register with SEC. Hester M. Peirce, Commissioner, Securities and Exchange Commission, "In the Matter of Poloniex, LLC." (Aug. 9, 2021).

[94]House Committee on Financial Services, Subcommittee on Digital Assets, Financial Technology, and Inclusion Subcommittee, *Coincidence or Coordinated? The Administration's Attack on the Digital Asset Ecosystem*,118th Cong. (Mar. 9, 2023); statement of Paul Grewal, Paul, Chief Legal Officer, Coinbase Global, Inc.

[95]Under Section 6(c) of the Securities Exchange Act, only registered broker-dealers may be admitted as members of a national securities exchange.15 U.S.C. § 78f(c).

[96]Gary Gensler, Chair, Securities and Exchange Commission, "Kennedy and Crypto," Sept. 8, 2022. The SEC Chair reiterated these views more recently in a June 2023 speech. See Gensler, Gary, Chair, Securities and Exchange Commission, "We've Seen This Story Before," Remarks before the Piper Sandler Global Exchange & Fintech Conference (June. 8, 2023).

crypto asset nonsecurities versus or alongside crypto asset securities.[97] However, he stated that the commingling of exchange, broker-dealer, custodial and other services within crypto asset intermediaries creates conflicts of interests and risks for investors that SEC does not allow in other marketplaces. He asked SEC staff to work with crypto asset intermediaries to ensure they register each of their functions, which could result in the intermediaries disaggregating these functions into separate legal entities to mitigate conflicts of interest and enhance investor protection.[98]

A former CFTC commissioner also raised questions as to how some crypto asset market participants could register as designated contract markets and comply with CFTC rules.[99] As of December 2022, CFTC had not issued further guidance or proposed rules providing additional clarification.

[97]In his speech, the SEC Chair also stated that to the extent CFTC needed greater authorities with which to oversee and regulate nonsecurity crypto asset tokens and related intermediaries, he looked forward to working with Congress to achieve that goal consistent with maintaining the regulation of crypto asset security tokens and related intermediaries at SEC. He stated that to the extent crypto asset intermediaries need to register with both SEC and CFTC, SEC currently has dual registrants (broker-dealers, fund advisors). We discuss gaps in regulatory authority over nonsecurity crypto asset spot markets later in this report.

[98]SEC has charged several prominent crypto asset trading platforms (and individuals associated them in some cases) for operating as an unregistered national securities exchange, broker, and clearing agency. In one complaint, SEC noted that the platform merged three functions that are typically separated in traditional securities markets. As examples, *see SEC v Bittrex, Inc., Bittrex Global GMBH, and William Hiroaki Shihara,* No. 2:23-cv-00580 (W.D.Wash filed April 17, 2023); *SEC v. Binance Holdings Limited, BAM Trading Services, Inc., BAM Management US Holdings Inc., and Changpeng Zhao*, No. 1:23-cv-01599, (D.D.C. filed June 5, 2023); and *SEC v. Coinbase, Inc. and Coinbase Global, Inc.*, No. 1:23-cv-04738, (S.D.N.Y. filed June 6, 2023).

[99]Dawn D. Stump, Commissioner, Commodity Futures Trading Commission, “We Can Do Hard Things” (Jan. 13, 2022).

Regulatory Gaps for Blockchain Products Increase Risks to Investors, Consumers, and Financial Stability

Gaps exist in regulatory authority over two key blockchain-related products we reviewed—crypto asset trading platforms and stablecoins. These gaps may compromise investor and consumer protection, market integrity, and financial stability. In addition, DeFi products and services could pose challenges for financial regulators.

Limited Federal Oversight of Spot Markets for Nonsecurity Crypto Assets Increases Fraud and Manipulation Risks

Federal regulators do not comprehensively oversee spot markets for crypto assets that are not securities for market integrity and investor protections, although participants in these markets are generally subject to registration and oversight by FinCEN for BSA/AML compliance purposes. As previously discussed, CFTC has limited authority to directly regulate commodity spot markets. FSOC noted that the spot markets for bitcoin and other nonsecurity crypto assets may not feature robust rules and regulations designed to ensure orderly and efficient trading, prevent conflicts of interest and market manipulation, and protect investors and the economy more broadly.[100] This stands in contrast to national securities exchanges and designated contract markets. Those markets are registered with SEC and CFTC, respectively, and are subject to requirements intended to protect investors and promote market integrity. For example, national securities exchanges and designated contract markets must adhere to

- requirements for listing securities or derivatives products, respectively, that will trade on the exchange; and
- rules and practices to prevent fraud, deception, or manipulation of trading on the exchange and of market prices for listed securities or

[100]Financial Stability Oversight Council, *Report on Digital Asset Financial Stability Risks and Regulation 2022* (Washington, D.C.: Oct. 3, 2022).

derivatives and to monitor trading to enforce compliance with these rules.[101]

Trading platforms that provide spot markets for crypto assets may be required to register as money transmitters under state law.[102] However, even in states that may regulate these trading platforms, money transmitter regulation may not comprehensively address market integrity issues and the potential for fraud, deception, or market manipulation on crypto asset trading platforms. Some states may provide more comprehensive regulation of crypto asset spot markets, but such oversight would apply only to those trading platforms licensed and operating in that state.[103]

A 2009 framework that we developed for evaluating regulatory reform proposals identifies several characteristics that should be reflected in a financial regulatory system.[104] One such characteristic is that the system

---

101Registered national securities exchanges are also self-regulatory organizations and must comply with regulatory requirements applicable to both national securities exchanges and SROs. 15 U.S.C. § 78c. Therefore, a national securities exchange generally sets standards of conduct for its members, coordinates with other self-regulatory organizations for the dissemination of consolidated market data, and generally takes responsibility for enforcing its own rules and provisions of the Exchange Act and regulations. Designated contract markets are also self-regulatory organizations and have obligations to monitor and enforce compliance with their rules. 7 U.S.C. § 7(d)(2); 17 C.F.R. § 38.150.

102Bloomberg Law, *Cryptocurrency Laws and Regulation by State* (May 26, 2022).

103For example, the New York Department of Financial Service requires that entities engaging in virtual currency activities seek a license (a BitLicense) to operate in the state or provide services to its residents or apply for a charter as a limited purpose trust company. The BitLicense applies to a wide range of virtual currency activities, including exchange services, which are defined as the conversion or exchange of (1) fiat currency or other value into virtual currency, (2) virtual currency into fiat currency or other value, or (3) one form of virtual currency into another form of virtual currency. Entities with a BitLicense must implement measures designed to effectively detect, prevent, and respond to fraud, attempted fraud, and similar wrongdoing. A limited purpose trust company can exercise fiduciary powers.

104Our 2009 framework for evaluating regulatory reform proposals describes nine characteristics that should be reflected in a financial regulatory system. The regulatory systems should (1) have clearly defined goals; (2) be appropriately comprehensive; (3) have systemwide focus; (4) be flexible and adaptable; (5) be efficient or effective; (6) allow for consistent consumer and investor protection; (7) provide regulators with independence, prominence, authority, and accountability; (8) provide for consistent financial oversight; and (9) limit minimal taxpayer exposure to financial risk. The framework is also used to craft proposals or revise existing proposals to make them more effective and appropriate for addressing the limitations of the current system. GAO-09-216.

be appropriately comprehensive. That is, financial regulations should cover all activities that pose risks or are otherwise important to meeting regulatory goals, such as consumer protection, by identifying risks and determining an appropriate oversight regime. Key actions to consider in determining the appropriate level of oversight for financial activities include closing statutory or regulatory gaps.

In addition, the CFTC Chairman and several commissioners from CFTC and SEC have stated that spot markets for commodity crypto assets should be subject to federal market regulation. In December 2022 Congressional testimony, the CFTC Chairman said that CFTC's current limited enforcement authority is no substitute for comprehensive regulation in which trading platforms and other critical infrastructure participants must register and be subject to direct oversight by a regulator such as CFTC.[105] He noted that by the time CFTC is able to exercise its anti-fraud and manipulation authority, it is already too late for defrauded customers. The CFTC Chairman previously stated that unlike most cash commodity markets, the market for crypto assets is characterized by a high number of retail investors mostly engaged in price speculation.[106]

FSOC also recommended that Congress pass legislation providing federal financial regulators with explicit rulemaking authority over spot markets for nonsecurity crypto assets. It noted that without appropriate regulation, spot markets for crypto assets could pose risks to the stability of the financial system if their interactions with the traditional financial system or their overall scale were to increase rapidly.[107] Several lawmakers have proposed legislation that would provide for federal oversight of these spot markets.[108]

[105]Senate Committee on Agriculture, Nutrition, and Forestry, *Why Congress Needs to Act: Lessons Learned from the FTX Collapse*, 117th Cong. (Dec. 1, 2022); statement of Chairman Rostin Behnam, Commodity Futures Trading Commission.

[106]Senate Committee on Agriculture, Nutrition, and Forestry, *Examining Digital Assets: Risks, Regulation, and Innovation*, 117th Cong. (Feb. 9, 2022); statement of Chairman Rostin Behnam, Commodity Futures Trading Commission.

[107]Financial Stability Oversight Council, *Report on Digital Asset Financial Stability Risks and Regulation 2022*.

[108]*See generally* Lummis-Gillibrand Responsible Financial Innovation Act, S.4356, 117th Cong. (2022); and Digital Commodity Exchange Act of 2022, H.R.7614, 117th Cong. (2022).

There has been some evidence of fraud and manipulation in the crypto asset spot market in recent years that suggests the market could benefit from additional regulation. For example, a 2020 academic study concluded that a single market manipulator on a prominent crypto asset trading platform likely fueled sizeable increases in Bitcoin prices between March 2017 and March 2018.[109] In addition, in March 2021, CFTC issued an order filing and settling charges against a prominent crypto asset trading platform for delivering false, misleading, or inaccurate reports concerning transactions in digital assets, including Bitcoin, on its electronic trading platform.[110]

More recently, the collapse and bankruptcy of FTX underscored the risks to investors from the lack of regulation over crypto asset spot markets. FTX operated a large crypto asset spot market overseas and a subsidiary crypto asset spot market in the United States. In his December 2022 testimony, the CFTC Chairman stated that if a regulator had had direct regulatory authority over crypto asset spot markets, FTX would have had to register with that regulator to operate in the United States. He said the regulator would have prohibited FTX from engaging in many of the activities that harmed investors and contributed to its collapse, including the commingling of customer and company accounts.

Crypto asset spot markets present risks for fraud and market manipulation, yet they provide fewer protections for retail investors than other markets that have significant retail participation. By designating a federal regulator to provide comprehensive federal oversight of spot markets for nonsecurity crypto assets, Congress could mitigate financial stability risks and better ensure that users of the platforms receive protections against fraud and market manipulation and protections that promote market integrity.

[109]John M. Griffin and Amin Shams, "Is Bitcoin Really Untethered?," *The Journal of Finance*, LXXV, no. 4 (August 2020).

[110]The order noted the platform was operating two trading programs—only one of which was disclosed—that generated orders that at times matched with one another. It then posted information from these transactions on its website and provided it to reporting services, resulting in a perceived volume and level of liquidity of digital assets that were false, misleading, or inaccurate. Coinbase Inc., CFTC No. 21-03, 2021 WL 1101461 (Mar. 19, 2021).

Stablecoins Lack Comprehensive and Consistent Oversight

Gaps in regulatory authority exist in the oversight of stablecoins, which raise consumer protection, safety and soundness, and financial stability concerns. Currently, stablecoins are not widely used to purchase goods and services outside of the crypto asset ecosystem, where they are primarily used to facilitate trading, lending, or borrowing of other crypto assets.

There are gaps in regulatory standards for stablecoins with respect to the composition of assets held in reserve, disclosures and audit requirements related to reserves, and redemption rights.

- Reserve asset composition. To maintain their promise that the coins can be redeemed at par on request, many stablecoin issuers advertise that the coins are backed by assets such as fiat currencies or financial instruments such as U.S. Treasury securities. A November 2021 report on stablecoins by the President's Working Group, OCC, and FDIC (PWG report) noted that there are no federal standards for the composition of stablecoin reserve assets.[111] It further noted that stablecoins differ in the riskiness of their reserve assets. Some stablecoin arrangements reportedly hold virtually all reserve assets in deposits at insured depository institutions or in U.S. Treasury securities.[112] Others reportedly hold riskier reserve assets, including commercial paper, corporate and municipal bonds, and other digital assets. Nonbank stablecoin issuers are also not subject to federal prudential standards, such as capital or liquidity requirements for issuing stablecoins and managing the reserve assets.
- Reserve disclosures and audit requirements. Although some stablecoin issuers voluntarily provide attestation reports about the nature of their reserves, there are no federal standards regarding audit requirements or public disclosures of reserve assets. In October 2021, CFTC settled charges against the largest stablecoin issuer for

[111]President's Working Group on Financial Markets, Federal Deposit Insurance Corporation, and Office of the Comptroller of the Currency, *Report on Stablecoins* (Washington D.C.: Nov. 1, 2021). The President's Working Group consists of the Secretary of the Treasury and the chairs of the Federal Reserve, SEC, and CFTC.

[112]A number of entities and activities are involved in the creation and management of a stablecoin, in what is referred to as a stablecoin arrangement. These activities can include governance, management of reserve assets, custody of reserve assets, settlement, and distribution.

misrepresenting the reserves it held against its token.[113] The PWG report and the Financial Stability Board also noted that any information made publicly available regarding an issuer's reserve assets is not consistent across stablecoin arrangements in terms of its content or the frequency of its release.[114]

- Redemption rights. There are no federal standards addressing redemption rights of stablecoin users. Stablecoin redemption rights can vary considerably, in terms of both who may present a stablecoin to an issuer for redemption and whether any limits exist on the quantity of coins that may be redeemed. The PWG report noted that some issuers are permitted under the terms of the arrangement to postpone redemption payments for 7 days, or even to suspend redemptions at any time. Some stablecoin issuers also differ in the nature of the claim provided to the user, with some providing a claim on the issuer and others providing no direct redemption rights to users.

Failure of a stablecoin to perform according to expectations could harm users of the stablecoin, particularly if users are uncertain about their ability to redeem the stablecoin in times of market stress. Facing the prospect that it could no longer maintain its value, holders of a stablecoin might believe they would be better off by redeeming their stablecoins earlier than others, setting off a "run." In a run on an asset-backed stablecoin, the stablecoin issuer might try to meet the redemption requests by liquidating reserve assets, potentially selling them at a discount. This could initiate a self-reinforcing cycle of further redemptions and the "fire sale" of reserve assets at greater discounts.

To the extent stablecoins become more integrated into the financial system and economy, their failures could have broader impacts on the economy and financial stability. According to the PWG report, runs on stablecoins could spread contagiously from one stablecoin to another, or

[113]CFTC found that the stablecoin issuer advertised it held $1 for every U.S.-dollar Tether token in circulation in a bank-held reserve, when in reality it did not hold sufficient reserves at all times to back the stablecoins in circulation. The order further found that the stablecoin issuer failed to disclose that it included unsecured receivables and nonfiat assets in its reserves, and falsely represented that it would undergo routine, professional audits to demonstrate that it maintained 100 percent reserves at all times although its reserves were not audited. Tether Holdings Ltd., Tether Operations Ltd., Tether Ltd., and Tether Int'l. Ltd., CFTC No. 22-04, 2021 WL 8322874 (Oct. 15, 2021).

[114]Financial Stability Board, *Assessment of Risks to Financial Stability from Crypto-assets.*

to other types of financial institutions that have a similar risk profile. FSOC noted in its October 2022 report on digital assets that traditional asset markets could experience dislocations if stablecoins were to obtain significant scale and if stablecoin runs were to lead to fire sales of assets held by other financial institutions that may be subject to runs, such as money market mutual funds.[115] However, the PWG report noted that risks to financial stability would be greater in the context of stablecoins backed by potentially volatile and illiquid assets than in the context of stablecoins backed one-for-one by high-quality liquid assets.

Stablecoin issuers are subject to the jurisdiction of multiple federal and state regulators, but the extent of their oversight varies and does not fully address the prudential risks posed by stablecoins. For example, SEC and CFTC have stated that, depending on their structure, stablecoins, or certain parts of stablecoin arrangements, may be securities, commodities, or derivatives and subject to their respective jurisdictions. Some stablecoin issuers are registered as money transmitters with the states. States impose requirements on licensed money transmitters—including restrictions on permissible investments—but states vary considerably in what they permit and state requirements generally are less restrictive than those for banks or money market mutual funds.[116]

Some stablecoin issuers have sought charters as trust banks under federal or state law, which may address some of the prudential risks associated with stablecoins, depending on the requirements. However, a representative of one stablecoin issuer noted that state-chartered trust

[115]Financial Stability Oversight Council, *Report on Digital Asset Financial Stability Risks and Regulation 2022*. A money market mutual fund invests in low-risk securities such as government securities, certificates of deposit, and commercial paper and aims to maintain a net asset value of $1 per share. Money market mutual funds are vulnerable to runs if customers lose faith in the adequacy of assets backing fund shares.

[116]*See* Dan Awrey, *Bad Money*, 106 Cornell L.Rev. 1, 47-54. (2020). Stablecoins that are backed by reserve assets have been compared to bank and money market mutual funds, largely because stablecoin issuers often promise that they can be redeemed in full on request and may invest customer funds in a range of financial assets. However, banks and money market mutual funds are subject to regulations intended to help bolster confidence in their ability to honor customers' redemption requests and limit the destabilizing effects of runs on both classes of institutions. As previously discussed, banks are subject to a comprehensive legal regime that includes capital and liquidity requirements, deposit insurance, access to emergency loans, and special resolution procedures. Money market mutual funds are not insured, but are subject to significant portfolio restrictions, transparency requirements, and liquidity rules.

banks are not recognized by all states and in those cases the entity still would need to obtain money transmitter licenses in the remaining states.

As previously discussed, one of our key principles for evaluating regulatory reform proposals is that a financial regulatory system should be appropriately comprehensive and cover all activities that pose risks or are otherwise important to meeting regulatory goals.[117] Another key principle is that a financial regulatory system should promote consistent financial oversight. That is, the system should ensure that similar institutions, products, risks, and services are subject to consistent regulation, oversight, and transparency, which should help minimize negative competitive outcomes while harmonizing oversight.

In its October 2022 report, FSOC recommended that Congress pass legislation to create a comprehensive federal prudential framework for stablecoin issuers.[118] Additionally, the PWG report identified legislative changes, including to regulators' authority, that are needed. Specifically, it recommended that Congress adopt legislation to address the prudential risks presented by stablecoin arrangements and concerns around redemption rights and reserves. The report recommended limiting stablecoin issuance and related issues of redemption and maintenance of reserve assets to insured banks.[119] The report noted that like other insured banks, those that issue stablecoins would be subject to (1) supervision and regulation by a federal banking agency, including consolidated supervision and regulation by the Federal Reserve at the holding company level; (2) capital and liquidity standards that are

[117] GAO-09-216.

[118] Financial Stability Oversight Council, *Report on Digital Asset Financial Stability Risks and Regulation 2022*.

[119] In the absence of Congressional action, the PWG report recommended that FSOC consider steps within its authority to address risks from stablecoins. This could include the designation of certain activities conducted within stablecoin arrangements as, or as likely to become, systemically important payment, clearing, and settlement activities. The report noted that designation would permit the appropriate agency to establish risk-management standards for financial institutions that engage in designated payment, clearing, and settlement activities. This could include requirements in relation to the assets backing the stablecoin, the operation of the stablecoin arrangement, and other prudential standards. The PWG report also made two recommendations for Congressional action to provide for (1) federal oversight over custodial wallet providers and any entity that performs activities critical to the functioning of the stablecoin arrangement and (2) restrictions limiting stablecoin issuers' affiliation with commercial entities and standards to promote interoperability among stablecoins. We did not examine these two recommendations because they were outside the scope of this report.

designed to address safety and soundness and, for the largest banking organizations, also include enhanced prudential standards that address financial stability concerns; and (3) a resolution regime that enables the orderly resolution of failed insured depository institutions.

Several lawmakers have introduced legislation to address the prudential risks associated with stablecoins.[120] While these proposals differ, most establish which institutions would be eligible to issue stablecoins, provide standards related to the composition of reserve assets and redemption rights, and impose disclosure and audit requirements. For example, several lawmakers proposed limiting stablecoin issuance to insured banks, while others also would permit issuance by federally licensed nonbanks. Additionally, many of the legislative proposals require insured banks or federally licensed nonbank stablecoin issuers to establish fully segregated reserves that hold only cash, cash equivalents, or other high-quality liquid assets with a market value at least equal to the par value of their outstanding stablecoins. Many would require stablecoin issuers to redeem stablecoins on demand.

By providing for consistent and comprehensive prudential regulation and oversight of stablecoin arrangements, Congress could better ensure that financial regulators are able to comprehensively and effectively address the risks these stablecoins can pose to consumers and investors, safety and soundness, and financial stability.

Financial Regulators May Face Challenges Overseeing Some DeFi Products and Services

Regulators' ability to address risks arising from DeFi products depends on their ability to apply regulation to these products or their issuers or operators. Federal financial regulators have applied regulations to DeFi products with some level of centralization. However, it is not clear how regulations will apply as DeFi products become more decentralized.

SEC and FinCEN staff told us they can apply regulation where they can identify individuals who are responsible for the development, operation, or governance of DeFi products and services. They noted most products and services advertised as DeFi are not fully decentralized since ownership and voting control may be concentrated in the hands of a few

[120]Examples of proposed legislation addressing stablecoins include the Stablecoin Classification and Regulation Act of 2020, H.R.8827, 116th Cong. (2020); Stablecoin Transparency Act, S.3970, H.R.7328, 117th Cong. (2022); Lummis-Gillibrand Responsible Financial Innovation Act, S.4356, 117th Cong. (2022); and the Stablecoin TRUST Act of 2022, S. 5340, 117th Cong. (2022).

investors. SEC and CFTC have brought enforcement actions against individuals who retained control over DeFi products. Examples include the following:

- In August 2021, SEC issued an order filing and settling charges against two men and their Cayman Islands-domiciled DeFi company for unregistered sales of more than $30 million of securities in unregistered offerings using smart contracts and DeFi technology. SEC found they made materially false and misleading statements concerning the operations and profitability of their business.[121]
- In January 2022, CFTC issued an order filing and settling charges against a DeFi trading platform for offering off-exchange, event-based binary options contracts (where the public could bet "yes" or "no" on a future event). The platform deployed smart contracts hosted on a blockchain to operate the market. According to the order, such event market contracts, each of which consists of a pair of binary options, constitute swaps under CFTC's jurisdiction, and therefore only can be offered on a registered exchange in accordance with the Commodity Exchange Act and CFTC regulations.[122]
- In September 2022, CFTC issued an order filing and settling charges against a DeFi firm and its two founders for creating and operating a blockchain-based software protocol that accepted orders for and facilitated margined and leveraged retail commodity transactions in digital assets without registering as a designated contract market or futures commission merchant and for failing to adopt a customer identification program as required by the Bank Secrecy Act.[123] The order found that the respondents subsequently transferred control of the software protocol to a decentralized autonomous organization—comprising governance token holders—that continued to operate the protocol in the same manner through its token holders. CFTC simultaneously filed a complaint charging the decentralized

[121]Blockchain Credit Partners D/B/A DeFi Money Market, Gregory Keough, and Derek Acree, Securities Act Release No. 10961, Securities Exchange Act Release No. 92588, SEC File No. 3-20453, 2021 WL 3470599 (Aug. 6, 2021).

[122]Blockratize, Inc. d/b/a Polymarket.com, CFTC No. 22-09, 2022 WL 73864 (Jan. 3, 2022).

[123]bZeroX, LLC; Tom Bean; and Kyle Kistner, CFTC No. 22-31, 2022 WL 4597664 (Sept. 22, 2022). Because the founders of the software protocol were voting members of the decentralized autonomous organization, CFTC found them liable for the law violations.

autonomous organization with violating the same laws as the respondents.[124]

However, it is not clear how regulations will apply when DeFi products become more decentralized and, consequently, how regulators can address the risks from these products. One former CFTC commissioner noted in a speech that in a mature peer-to-peer DeFi system, no intermediary monitors markets for fraud and manipulation, prevents money laundering, safeguards deposited funds, ensures counterparty performance, or makes consumers whole when processes fail.[125]

Similarly, FinCEN staff noted that if financial institutions or other intermediaries with BSA obligations are completely removed from transactions, illicit finance risk increases as a result of less reporting to FinCEN and fewer preventative measures to curb criminals from moving money. FinCEN staff said they have been evaluating how BSA/AML regulation might be applied to truly decentralized platforms.[126]

The risks associated with DeFi products and services increase as they become interconnected. As previously discussed, the open source code underlying DeFi allows protocols to be layered to create financial services and instruments that are not available from any single product or service. According to a Federal Reserve staff study on DeFi, a financial shock or operational failure of one DeFi protocol may spread through DeFi connections to other products and amplify the risks to consumers.[127]

[124]CFTC charged the Ooki DAO with operating an illegal trading platform and unlawfully acting as a futures commission merchant. On June 8, 2023, the District Court entered a default judgment against the Ooki DAO and ordered permanent trading and registration bans. *CFTC v. Ooki DAO,* Civil Action No: 3:22-cv-05416-WHO (N.D. Cal. June 8, 2023).

[125]“Climate Change and Decentralized Finance: New Challenges for the CFTC,” keynote address of Commissioner Dan M. Berkovitz, Commodity Futures Trading Commission, at the Asset Management Derivatives Forum 2021 of the Futures Industry Association and Securities Industry and Financial Markets Association-Asset Management Group (June 8, 2021).

[126]FinCEN staff noted they have some visibility into DeFi transactions. DeFi transactions are pseudonymous, as are other cryptocurrency transactions, but they can still be tracked and traced and in specific instances attributed to real-world persons.

[127]Francesca Carapella, et al., “Decentralized Finance (DeFi): Transformative Potential & Associated Risks.”

To the extent DeFi products become widespread and link to traditional financial institutions, operational or financial shocks could have implications for the broader financial system. FSOC noted in its 2021 annual report that links between traditional financial institutions, markets, and infrastructure to various digital assets and DeFi projects may create a channel for a risk event in digital assets to spread to the broader financial system. A study by Bank of International Settlement staff noted that increased connections between DeFi and the traditional financial system would increase the potential for spillover effects to banks and nonbank institutions.[128]

The risks associated with mature DeFi products likely will span multiple regulatory jurisdictions, especially as developers layer DeFi protocols to create products that offer multiple types of financial services. One DeFi company representative told us that mature DeFi protocols that span multiple regulatory jurisdictions currently are on the market. Another DeFi company representative said that a single product—either one protocol or an application built on a composition of multiple available protocols—could offer trading in swaps and derivatives contracts and offer lending and borrowing services. As discussed below, a coordinated response among agencies could help to address the potential risks of these products.

Regulators Lack an Ongoing Coordination Mechanism for Addressing Blockchain Risks in a Timely Manner

Addressing emerging and sometimes novel risks from blockchain-related products and services requires regulators to take action not only within their jurisdictions, but also across jurisdictions. However, the financial regulators' coordination efforts have not resulted in timely action to identify regulatory responses to blockchain risks that span multiple jurisdictions.

For example, FSOC first identified the financial stability concerns associated with stablecoins in its December 2019 annual report.[129] However, FSOC did not promptly follow its identification of risk with a response identifying how it could address these risks, such as by proposing legislation or invoking its payment, clearing, and settlement designation authority. Federal financial regulators (working through PWG) did not respond to these risks until the November 2021 issuance of the

128Sirio Aramonte, Wenqian Huang, and Andreas Schrimpf, "DeFi risks and the decentralisation illusion," *BIS Quarterly Review* (December 2021).

129Financial Stability Oversight Council, *2019 Annual Report* (Washington, D.C.: 2019).

PWG report in which they recommended legislative action. FSOC then followed with responses in an October 2022 report, which we discuss in more detail in the following pages.[130] Individual regulators and FSOC also identified risks related to DeFi, as discussed earlier, but have not yet collectively identified potential regulatory responses, including any cross-cutting or coordinated actions, to address these risks.

Federal financial regulators told us that the rapid pace of blockchain innovation makes it challenging to keep regulation up to speed. Representatives of crypto asset trading platforms, DeFi companies, stablecoin issuers, and a blockchain association told us that federal financial regulators have been slow to identify and clarify how regulation applies to blockchain-related products and services. Those representatives said the slow regulatory response hindered innovation and has driven some companies abroad. They said some blockchain companies avoid the U.S. market because of its regulatory uncertainty, noting they can develop and deploy their products more quickly in other countries that provide more certainty.

Our 2009 framework for evaluating regulatory reform proposals identifies characteristics that should be reflected in a financial regulatory system, including that they be flexible and forward-looking, allowing regulators to readily adapt to market innovations and act on emerging risks in a timely way without hindering innovation.[131]

The federal financial regulators have stressed the importance of coordination in building and adapting regulatory frameworks for blockchain-related products and services. In an August 2021 Congressional testimony, the Acting Comptroller of the Currency said that financial regulators must collectively adapt to the digitalization of banking and finance.[132] However, he expressed concern that the regulatory community was taking a fragmented, agency-by-agency approach in adapting the regulatory framework to the digital asset space. He noted that to the extent interagency coordination existed, it tended to be tactical

[130]Financial Stability Oversight Council, *Report on Digital Asset Financial Stability Risks and Regulation* (Washington, D.C.: Oct. 3, 2022).

[131]GAO-09-216.

[132]Senate Committee on Banking, Housing and Urban Affairs, *Oversight of Regulators: Does Our Financial System Work for Everyone?*, 117th Cong. (Aug. 3, 2021); statement by Michael J. Hsu, Acting Comptroller of the Currency.

and focused on a pressing issue and did not reflect an overarching strategy. In February 2022, a Treasury official said it is critical that regulatory frameworks are in place for both traditional and digital native financial intermediaries that appropriately address risks. She noted that regulators' crypto policy sprint and the President's Working Group were important steps in this direction but that much more work remained to be done.[133]

The March 2022 Executive Order on Ensuring Responsible Development of Digital Assets directed federal agencies to create a unified approach on regulation and oversight of crypto assets. The order directed Treasury, in consultation with federal financial regulators and other agencies, to produce a report that identified the risks of crypto assets to consumers, investors, and businesses. It also directed the Treasury Secretary to convene FSOC to produce a report identifying the risks of crypto assets to financial stability. It directed FSOC and Treasury to identify recommendations for addressing the identified risks and implications, including proposals for additional adjusted regulation and supervision, as well as new legislation.

In their respective reports, both Treasury and FSOC recommended that regulators work collaboratively to address the risks identified. Treasury's September 2022 report recommended that U.S. regulatory agencies work collaboratively to promote consistent and comprehensive oversight of crypto assets.[134] It also recommended that, as appropriate, the agencies work together to review existing regulations and clarify regulatory requirements applicable to crypto asset products and services. FSOC's October 2022 report recommended that federal financial regulators coordinate in their crypto asset supervision to address issues related to regulatory arbitrage or the lack of a single regulator having visibility across all of an entity's affiliates.[135]

However, regulators' formal coordination mechanisms do not regularly convene specifically to identify the full range of risks and regulatory

---

133Senate Committee on Banking, Housing and Urban Affairs, *Examining the President's Working Group on Financial Markets Report on Stablecoins*, 117th Cong. (Feb. 15, 2022); statement by Jean Nellie Liang, Under Secretary for Domestic Finance, Department of the Treasury.

134Department of the Treasury, *Crypto-Assets: Implications for Consumers, Investors, and Businesses* (Washington, D.C.: Sept. 16, 2022).

135Financial Stability Oversight Council, *Report on Digital Asset Financial Stability Risks and Regulation*.

challenges of existing and emerging blockchain products and services and provide a timely response to any unaddressed risks. Such responses could include industry guidance, proposed regulation, or recommendations to Congress for legislation. Regulators have engaged in some coordination to respond to blockchain risks, but these efforts have been targeted towards specific products, such as stablecoins, or a type of regulated entity, such as banks. Furthermore, these efforts are neither ongoing nor do they include the seven federal financial regulators that were the focus of this review. Additionally, the scope of coordination through FSOC is limited to potential financial stability risks.

Our prior work on collaborative mechanisms found that agencies can strengthen their commitment to working collaboratively by articulating their agreements in formal documents, such as a memorandum of understanding, interagency guidance, or an interagency planning document.[136] A formal interagency planning document could facilitate the efforts of the financial regulators to respond to blockchain-related risks in a timely manner. For example, such a document could establish processes for identifying risks and responding to them within agreed-upon time frames.

Establishing or adapting an existing formal coordination mechanism for addressing issues related to blockchain-related products would help ensure that federal financial regulators collectively identify risks posed by blockchain-related products and services and develop and implement regulatory responses in a timely manner. In turn, this could improve protections for consumers and investors, mitigate illicit finance and threats to financial stability, and promote responsible innovation and U.S. competitiveness.

Conclusions

As markets for crypto assets and other blockchain-related products and services have grown, so has the need for federal financial regulators to address the risks they pose to consumers, investors, and financial stability. Recent market turmoil and instances of fraud related to crypto assets, stablecoins, and trading platforms illustrate the significant risks to consumers and investors. And the potential for risks to financial stability will increase as blockchain products and services continue to grow and integrate into the mainstream financial system.

[136] GAO, *Results-Oriented Government: Practices That Can Help Enhance and Sustain Collaboration among Federal Agencies*, GAO-06-15 (Washington, D.C.: Oct. 21, 2005).

However, gaps in regulators' authority limit their ability to effectively mitigate these risks:

- First, trading platforms that serve as spot markets for nonsecurity crypto assets are generally narrowly regulated—they may be overseen by states in the context of money transmitter regulation and federally by FinCEN for BSA/AML oversight. As a result, they may not be subject to requirements intended to protect investors from fraud and market manipulation and to promote market integrity. By providing for more comprehensive federal oversight of spot markets for nonsecurity crypto assets, Congress could better ensure that users of the platforms receive such protections.
- Second, there are gaps in regulatory authority over prudential risks posed by stablecoins. Issues that we and others identified include the limited public information available on reserve assets, the extent of redemption rights, and inconsistent or lacking capital and liquidity requirements. By providing for consistent and comprehensive oversight of stablecoins, Congress could better ensure protections for consumers, investors, and markets. For instance, such legislation could establish which institutions are eligible to issue stablecoins. Other elements of such legislation could establish or provide for minimum requirements related to the composition of reserve assets, public disclosure and regular audits of reserve assets and audit results, and prudential standards.

The rapid pace of change that marks blockchain underscores the importance of a coordinated response by federal regulators. Yet regulators' coordination efforts to date have not always addressed risks posed by crypto assets in a timely manner. Establishing or adapting an existing formal coordination mechanism for addressing blockchain-related products and services could help federal financial regulators collectively identify risks and develop appropriate regulatory responses, and to do so in a timely manner. In turn, this could improve protections for consumers and investors, mitigate illicit finance and threats to financial stability, and promote responsible innovation and U.S. competitiveness.

Matters for Congressional Consideration

We are recommending the following two matters for congressional consideration:

Congress should consider legislation that designates a federal regulator to provide for comprehensive regulatory oversight of spot markets for nonsecurity crypto assets, including requirements intended to protect investors from fraud and market manipulation and to promote market integrity. (Matter for Consideration 1)

Congress should consider legislation providing for consistent and comprehensive oversight of stablecoin arrangements. Such legislation might include provisions identifying which institutions are eligible to issue such stablecoins; establishing minimum requirements for the composition of reserve assets and requirements for regular audits of and public disclosures of reserve assets and audit results; establishing prudential standards; and establishing redemption rights. (Matter for Consideration 2)

Recommendations for Executive Action

We are making a total of seven recommendations (one each) to CFPB, CFTC, FDIC, the Federal Reserve, NCUA, OCC, and SEC:

The Director of the Consumer Financial Protection Bureau should jointly establish or adapt an existing formal coordination mechanism with CFTC, FDIC, the Federal Reserve, NCUA, OCC, and SEC for collectively identifying risks posed by blockchain-related products and services and formulating a timely regulatory response. To facilitate these objectives, this mechanism could include formal planning documents that establish the frequency of meetings and processes for identifying risks and responding to them within agreed-upon time frames. (Recommendation 1)

The Chairman of the Commodity Futures Trading Commission should jointly establish or adapt an existing formal coordination mechanism with CFPB, FDIC, the Federal Reserve, NCUA, OCC, and SEC for collectively identifying risks posed by blockchain-related products and services and formulating a timely regulatory response. To facilitate these objectives, this mechanism could include formal planning documents that establish the frequency of meetings and processes for identifying risks and responding to them within agreed-upon time frames. (Recommendation 2)

The Chairman of the Federal Deposit Insurance Corporation should jointly establish or adapt an existing formal coordination mechanism with CFPB, CFTC, the Federal Reserve, NCUA, OCC, and SEC for collectively identifying risks posed by blockchain-related products and services and formulating a timely regulatory response. To facilitate these objectives, this mechanism could include formal planning documents that establish the frequency of meetings and processes for identifying risks and responding to them within agreed-upon time frames. (Recommendation 3)

The Chair of the Board of Governors of the Federal Reserve System should jointly establish or adapt an existing formal coordination mechanism with CFPB, CFTC, FDIC, NCUA, OCC, and SEC for collectively identifying risks posed by blockchain-related products and services and formulating a timely regulatory response. To facilitate these objectives, this mechanism could include formal planning documents that establish the frequency of meetings and processes for identifying risks and responding to them within agreed-upon time frames. (Recommendation 4)

The Chairman of the National Credit Union Administration should jointly establish or adapt an existing formal coordination mechanism with CFPB, CFTC, FDIC, the Federal Reserve, OCC, and SEC for collectively identifying risks posed by blockchain-related products and services and formulating a timely regulatory response. To facilitate these objectives, this mechanism could include formal planning documents that establish the frequency of meetings and processes for identifying risks and responding to them within agreed-upon time frames. (Recommendation 5)

The Comptroller of the Currency should jointly establish or adapt an existing formal coordination mechanism with CFPB, CFTC, FDIC, the Federal Reserve, NCUA, and SEC for collectively identifying risks posed by blockchain-related products and services and formulating a timely regulatory response. To facilitate these objectives, this mechanism could include formal planning documents that establish the frequency of meetings and processes for identifying risks and responding to them within agreed-upon time frames. (Recommendation 6)

The Chairman of the Securities and Exchange Commission should jointly establish or adapt an existing formal coordination mechanism with CFPB, CFTC, FDIC, the Federal Reserve, NCUA, and OCC for collectively identifying risks posed by blockchain-related products and services and formulating a timely regulatory response. To facilitate these objectives, this mechanism could include formal planning documents that establish the frequency of meetings and processes for identifying risks and responding to them within agreed-upon time frames. (Recommendation 7)

Agency Comments and Our Evaluation

We provided a draft of this report to CFPB, CFTC, the Federal Reserve, FDIC, FinCEN, FSOC, NCUA, OCC, Office of Domestic Finance, OFR, and SEC for review and comment. CFPB, CFTC, the Federal Reserve, FDIC, FinCEN, OCC, Office of Domestic Finance, and SEC provided technical comments, which we incorporated as appropriate. CFPB, the Federal Reserve, FDIC, NCUA, OCC, and SEC also provided written comments, which are reproduced in appendixes II–VII. NCUA agreed with our recommendation and CFPB, the Federal Reserve, FDIC, OCC, and SEC neither agreed nor disagreed. In their written comments, CFPB, the Federal Reserve, FDIC, OCC, and SEC noted they have coordinated through venues including FSOC, the President's Working Group, Financial Literacy Education Committee, and some international organizations. The Federal Reserve, FDIC, and OCC said they have identified risks posed by blockchain-related products and services through existing coordination mechanisms.

We recognize that the federal financial regulators have coordinated through various venues, and identified unaddressed risks related to crypto assets and, in some cases, responses to those risks. However, regulators' coordination efforts to date have not always addressed risks posed by crypto assets in a timely manner. We maintain that a formal coordination mechanism focused on collectively identifying risks posed by blockchain-related products and services and formulating timely regulatory responses could improve protections for consumers and investors, mitigate illicit finance and threats to financial stability, and promote responsible innovation and U.S. competitiveness. In response to comments from CFPB, CFTC, FDIC, and SEC, we modified our recommendation to acknowledge that such a coordination mechanism could be established through a new or existing venue.

In its written comment letter, SEC said that it did not agree with all the positions in the report regarding the crypto industry's risks. As we noted, the risks and potential benefits we include in the first section of the report are not intended to be comprehensive and do not represent the complete perspective of any one entity. Rather, they are an aggregate list of key risks and potential benefits, constructed by reviewing industry, government, and third-party reports and with input from industry representatives, consumer advocacy organizations, and staff from each of the federal financial regulators that we interviewed.

SEC also said that it did not agree with all of our positions regarding the applicability of federal securities laws to aspects of the crypto industry. We did not take a position on whether specific crypto assets or crypto assets more broadly are securities, an issue that is subject to litigation. In the report, we discuss SEC officials' statements that many crypto assets are likely securities and that many crypto asset platforms are trading these securities without registering as a national securities exchange.

We also discuss the views of other federal financial regulators as to gaps in regulatory authority over spot markets for nonsecurity crypto assets and stablecoins. Specifically, we discuss FSOC's October 2022 report recommendation that Congress pass legislation providing federal financial regulators with explicit rulemaking authority over spot markets for nonsecurity crypto assets and the CFTC Chairman's statements that these spot markets should be subject to federal market regulation. We also discuss FSOC's recommendation that Congress pass legislation to create a comprehensive federal prudential framework for stablecoin issuers and the November 2021 PWG report's similar recommendation that Congress adopt legislation to address the prudential risks presented by stablecoin arrangements and concerns around redemption rights and reserves.

In response to SEC's technical comments, we included more recent statements from the SEC Chair. We discussed a September 2022 speech in which the SEC Chair reiterated his view that most crypto assets are securities because they are investment contracts under the *Howey* test. He also stated that SEC provided guidance to the industry for determining whether a crypto asset is a security under federal securities laws, including through the 2017 DAO report, SEC enforcement actions, and the 2019 SEC staff framework for investment contract analysis.

We also included the SEC Chair's statements that the commingling of exchange, broker-dealer, custodial and other services in crypto asset intermediaries creates conflicts of interests and risks for investors that SEC does not allow in other marketplaces. We noted that he asked SEC staff to work with such intermediaries to ensure they register each of their functions, which could result in the intermediaries disaggregating these functions into separate legal entities to mitigate conflicts of interest and enhance investor protection.

As agreed with your offices, unless you publicly announce the contents of this report earlier, we plan no further distribution until 30 days from the report date. At that time, we will send copies of this report to the appropriate congressional committees, the Director of the Consumer Financial Protection Bureau, Chairman of the Commodity Futures Trading Commission, Chairman of the Federal Deposit Insurance Corporation, Chair of the Board of Governors of the Federal Reserve System, Acting Director of the Financial Crimes Enforcement Network, Chairman of the National Credit Union Administration, Acting Comptroller of the Currency, Chairman of the Securities and Exchange Commission, Secretary of the Treasury as the Chairperson of FSOC and in her leadership role for OFR and Office of Domestic Finance, and other interested parties. The report will also be available at no charge on our website at http://www.gao.gov.

If you or your staff have any questions about this report, please contact me at (202) 512-8678 or clementsm@gao.gov. Contact points for our Offices of Congressional Relations and Public Affairs are listed on the last page of this report. GAO staff who made major contributions to this report are listed in appendix VIII.

Michael E. Clements
Director, Financial Markets and Community Investment

Appendix I: Objectives, Scope, and Methodology

This report examines (1) key blockchain-related financial products and services, including their potential benefits and risks; (2) federal financial regulators' jurisdiction over blockchain-related products and services; (3) gaps in regulatory authority; and (4) regulators' coordination on and response to risks posed by blockchain-related products and services.

To address our first objective, we reviewed prior GAO reports and reports from federal financial regulators, international financial regulatory associations, industry associations representing banks and blockchain-related financial service companies, crypto industry research organizations, and consulting firms. Using these sources, we identified key blockchain-related financial products and services, categories for those products and services, and associated benefits and risks. Two blockchain industry associations, a crypto industry research organization, and federal financial regulators reviewed and provided feedback on our categorization of blockchain-related financial products and services and the associated benefits and risks, and we incorporated that feedback as appropriate.

To address our second objective, we reviewed and analyzed prior GAO reports; Congressional Research Service reports; relevant laws and regulations; federal financial regulator reports, guidance, speeches, and enforcement actions; and studies from international financial regulatory bodies and crypto industry research organizations. We reviewed these documents to identify each financial regulator's jurisdiction as it relates to blockchain-related products and services.

To address our third objective, we selected three blockchain-related product and service categories to examine for gaps in regulatory authority: crypto asset trading platforms, stablecoins, and decentralized finance products and services. We selected these three categories because of their rapid growth, exposure to retail customers, and the potential risks they pose to consumers, investors, and the financial system. To make this selection, we reviewed prior GAO reports; reports from federal financial regulators, international financial regulatory associations, industry associations representing banks and blockchain-related financial service companies, crypto industry research organizations, and consulting firms; and speeches by federal financial regulators. To identify any gaps in regulators' authority and challenges faced by regulators, we reviewed and analyzed the documents described above. We assessed federal regulatory oversight of the three blockchain-related products and services against GAO's 2009 framework for crafting and assessing proposals to modernize the U.S financial regulatory system.[1]

For the fourth objective, we reviewed federal financial regulator reports, guidance, and speeches, such as the President's Working Group, Federal Deposit Insurance Corporation, and the Office of the Comptroller of the Currency's report on stablecoins; the March 2022 Executive Order on Ensuring Responsible Development of Digital Assets; and the federal banking regulators' joint statement on the policy sprint initiative for crypto assets. We also reviewed information obtained from our regulatory gap analyses as part of the third objective. In our review of these documents, we identified federal financial regulators' coordination efforts related to blockchain-related products and services, assessed the extent to which those efforts addressed regulatory gaps or challenges identified in our third objective, and identified coordination elements that would better enable regulators to address regulatory gaps and challenges. We assessed these coordination efforts against our 2009 framework. We also assessed these coordination efforts against coordination recommendations from Department of the Treasury and Financial Stability Oversight Council reports on blockchain regulation in fall 2022.

For the third and fourth objectives, we conducted three group discussions with a nonrandom selection of firms offering or representing (1) crypto asset trading platforms, (2) stablecoin issuers, and (3) decentralized finance companies (one discussion group for each category). We identified firms to participate in these discussions by reviewing industry publications, reports, and public remarks issued by blockchain-related companies, law firms, and crypto industry research organizations that discussed the size, relevance, or position of particular firms in the blockchain sphere. From among this list, we selected firms that represented a range of business models, were recognized as industry leaders, or previously publicly commented on the regulation of trading platforms, stablecoins, or decentralized finance.

For the discussion group on crypto asset trading platforms, we selected four firms, which consisted of one law firm and three platforms that trade crypto assets. For the stablecoin group, we selected two firms—a

[1]GAO, *Financial Regulation: A Framework for Crafting and Assessing Proposals to Modernize the Outdated U.S. Financial Regulatory System*, GAO-09-216 (Washington, D.C.: Jan. 8, 2009). To develop this framework, we synthesized existing GAO work and other studies and met with dozens of representatives of financial regulatory agencies, industry associations, consumer advocacy organizations, and others.

stablecoin issuer and a law firm. We also separately interviewed another stablecoin issuer that was unable to attend the group discussion. For the final group, we selected four decentralized finance companies, representing lending, derivatives, and crypto trading platforms. In these interviews, we discussed participants' experiences with regulation of blockchain products and services, the extent to which regulation supports or creates challenges to innovation, and the extent of regulatory gaps or a need for regulatory clarification.

For all four objectives, we interviewed officials from the following federal financial regulatory agencies and entities: Commodity Futures Trading Commission, Securities and Exchange Commission, Federal Deposit Insurance Corporation, Board of Governors of the Federal Reserve System, Office of the Comptroller of the Currency, Consumer Financial Protection Bureau, National Credit Union Administration, and entities and offices in the Department of the Treasury (Financial Stability Oversight Council, Financial Crimes Enforcement Network, Office of Financial Research, and Office of Domestic Finance).

We also interviewed officials of two self-regulatory organizations (Financial Industry Regulatory Authority and National Futures Association); state regulatory associations and state regulators (Conference of State Bank Supervisors, North American Securities Administrators Association, and Money Transmitter Regulators Association), and financial regulatory agencies from Wyoming and New York, which both have explicit frameworks for crypto asset activities.

Additionally, we interviewed two industry associations representing banking and traditional finance (American Bankers Association and Securities Industry and Financial Markets Association); two blockchain-related financial services associations (Blockchain Association and Wall Street Blockchain Alliance); and two consumer advocacy organizations (American Association of Individual Investors and Americans for Financial Reform). Finally, we interviewed researchers from the Brookings Institute, a think tank, and from Coincenter, a crypto-industry research organization.

We conducted this performance audit from July 2021 to June 2023 in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

Appendix II: Comments from Consumer Financial Protection Bureau

cfpb Consumer Financial Protection Bureau

1700 G Street NW, Washington, D.C. 20552

February 3, 2023

Michael E. Clements
Director
Financial Markets and Community Investment
Government Accountability Office
441 G Street, NW
Washington DC, 20548

Dear Mr. Clements,

Thank you for the opportunity to review and comment on the draft report by the Government Accountability Office (GAO), titled *Blockchain in Finance: Legislative and Regulatory Actions Needed to Ensure Comprehensive Oversight of Crypto Assets* (GAO-23-105346). The report examines the benefits and risks of blockchain-based financial products and services; the financial regulatory structure as it applies to these applications; and the federal government's coordination efforts in this space.

In the report, GAO makes seven recommendations for executive action, one of which is directed to the Consumer Financial Protection Bureau (CFPB). GAO recommends that the CFPB "jointly establish" with the Commodity Futures Trading Commission (CFTC), Federal Deposit Insurance Corporation (FDIC), Board of Governors of the Federal Reserve System (Federal Reserve Board), National Credit Union Administration (NCUA), Office of the Comptroller of the Currency (OCC), and Securities and Exchange Commission (SEC) a "formal coordination mechanism for collectively identifying risks posed by blockchain-based products and services and formulating a timely regulatory response." GAO also recommends that to "facilitate these objectives," the jointly established coordination mechanism "could include formal planning documents that establish the frequency of meetings and processes for identifying risks and responding to them within agreed-upon timeframes."

consumerfinance.gov

The CFPB recognizes the importance of working collaboratively with its fellow regulators in addressing blockchain-based consumer financial products and services. To that end, the CFPB has been coordinating with its fellow members on the Financial Stability Oversight Council (FSOC) and Financial Literacy and Education Commission (FLEC), including the CFTC, FDIC, Federal Reserve Board, NCUA, OCC, and SEC.[1] Indeed, both the FSOC and FLEC have created sub-groups specifically focused on crypto-assets. Additionally, as GAO's report recognizes, in response to a recommendation from the U.S. Department of the Treasury's September 2022 report entitled *Crypto-Assets: Implications for Consumers, Investors, and Businesses*, the FLEC, where the CFPB serves as Vice-Chair, is working to ensure that U.S. consumers, investors, and businesses have access to trustworthy information on crypto-assets.

The CFPB is committed to continuing and strengthening its coordination efforts to reduce risks posed by crypto-assets to consumers and ensure that consumers have access to unbiased, reliable information.

Sincerely,

Rohit Chopra

Rohit Chopra
Director

[1] The CFPB also coordinates with the FDIC, Federal Reserve Board, NCUA, and OCC through the Federal Financial Institutions Examination Council.

Appendix III: Comments from the Board of Governors of the Federal Reserve System

BOARD OF GOVERNORS OF THE FEDERAL RESERVE SYSTEM
WASHINGTON, D. C. 20551

DIVISION OF
SUPERVISION AND REGULATION

February 2, 2023

Michael E. Clements, Director
Financial Markets and Community Investment Team
United States Government Accountability Office
441 G Street, NW
Washington, DC 20548

Dear Mr. Clements:

Thank you for providing the Board of Governors of the Federal Reserve System ("Board") with an opportunity to review the final draft of the Government Accountability Office ("GAO") report titled: *Blockchain in Finance: Legislative and Regulatory Actions Needed to Ensure Comprehensive Oversight of Crypto Assets* (GAO-23-105346). The GAO's report reviews the use of blockchain-based financial products and services and their associated risks and benefits, as well as the oversight of the providers of blockchain-based products and services by the federal financial regulators. We appreciate the report's recognition of the federal banking regulators' efforts to understand the current and potential uses of crypto-assets and distributed ledger technology and related risks and identify areas where further regulatory guidance or clarity may be warranted.

The GAO's report makes one recommendation to the Board:

> The Chair of the Board of Governors of the Federal Reserve System should jointly establish with CFPB, CFTC, FDIC, NCUA, OCC, and SEC a formal coordination mechanism for collectively identifying risks posed by blockchain-based products and services and formulating a timely regulatory response. To facilitate these objectives, this mechanism could include formal planning documents that establish the frequency of meetings and processes for identifying risks and responding to them within agreed-upon timeframes.

The Board recognizes the importance of a coordinated and timely agency

www.federalreserve.gov

2

response in identifying and addressing potential risks posed by use of blockchain technology and blockchain-based products and services. To that end, the Board routinely and frequently engages in collaborative discussions with the CFPB, CFTC, FDIC, NCUA, OCC, and SEC on various issues related to emerging risks, including those related to blockchain-based products and services. For example, the Financial Stability Oversight Council recently published a report on digital assets and financial stability risks and regulation, which identifies vulnerabilities associated with digital assets and makes recommendations to address gaps in the regulatory framework. These vulnerabilities and recommendations were also highlighted in the Financial Stability Oversight Council's Annual Report.[1] Additionally, the Board works with the other federal banking agencies on issues regarding banking organizations seeking to engage in activities involving blockchain technology and crypto-assets, including identifying and appropriately responding to related risks within each agency's respective authority. To that end, on January 3, 2023, the Board, FDIC, and OCC issued a joint statement highlighting key risks of crypto-assets for banking organizations.[2] The Board has also developed a process for banking organizations to engage in robust supervisory discussions with Federal Reserve staff around proposed or existing crypto-asset related activities and their associated risks, which is aligned with processes developed by the FDIC and the OCC. In addition, the agencies routinely collaborate when participating in multiple international groups that are developing principles and standards for the use of blockchain technology in financial services.[3] In light of these existing effective collaborative efforts and with respect to the GAO's recommendation, the Board will consider ways to collaborate, through existing or new coordination mechanisms, with the CFPB, CFTC, FDIC, NCUA, OCC, and SEC to collectively detect and address the risks and challenges presented by the use of blockchain technology and related products and services.

We appreciate the GAO's review of blockchain technology in financial services, for their professional approach to the review, and for the opportunity to comment.

Sincerely,

Michael Gibson
Director

[1] *See* https://home.treasury.gov/system/files/261/FSOC-Digital-Assets-Report-2022.pdf and https://home.treasury.gov/system/files/261/FSOC2022AnnualReport.pdf.
[2] *See* https://www.federalreserve.gov/newsevents/pressreleases/bcreg20230103a.htm.
[3] *See, e.g.,* https://www.bis.org/bcbs/publ/d545.htm.

Appendix IV: Comments from Federal Deposit Insurance Corporation

FDIC

Federal Deposit Insurance Corporation
550 17th Street NW, Washington, D.C. 20429-9990 Division of Risk Management Supervision

February 3, 2023

Michael Clements
Director
Financial Markets and Community Investment
U.S. Government Accountability Office
441 G Street, NW
Washington, D.C. 20548

Dear Mr. Clements:

The Federal Deposit Insurance Corporation (FDIC) appreciates the opportunity to review the GAO draft report *Blockchain in Finance – Legislative and Regulatory Actions Needed to Ensure Comprehensive Oversight of Crypto Assets* (Report) (GAO-23-105346). The Report examines the regulatory framework for the use of blockchain in the financial sector.

The Report contains one recommendation to the FDIC, along with a similar recommendation to other regulators. The Report recommends that the "Chairman of the Federal Deposit Insurance Corporation should jointly establish with CFPB, CFTC, Federal Reserve, NCUA, OCC, and SEC a formal coordination mechanism for collectively identifying risks posed by blockchain-based products and services and formulating a timely regulatory response. To facilitate these objectives, this mechanism could include formal planning documents that establish the frequency of meetings and processes for identifying risks and responding to them within agreed-upon timeframes."

The FDIC recognizes the importance of coordination with fellow regulators to understand risks and, when appropriate, coordinate on a regulatory response. To that end, the FDIC participates in a number of existing coordination mechanisms, both domestically and internationally, to address the risks of banks engaging in blockchain-based crypto-asset related activities, and to provide regulatory responses where appropriate.

However, it is important to note that the recommendation relates to identifying and responding to risks posed by blockchain-based products and services. The FDIC does not have statutory authority over products and services. Rather, the FDIC's authorities are related to insured financial institutions, and in particular, the FDIC is the primary federal regulator for state non-member banks and state savings associations. This is an important distinction because the FDIC's current collaboration efforts and venues with other regulators relative to crypto-asset related activities depend on several factors for a particular risk topic, including authorities and jurisdiction.

Mr. Clements, Director

As mentioned in the Draft Report, the FDIC participated in the President's Working Group development of a paper on payment stablecoins. In addition, the FDIC has been coordinating with the Financial Stability Oversight Council (FSOC)[1], which has created a working group specifically focused on crypto-assets. The FDIC is also a member of the Basel Committee on Banking Supervision,[2] which has addressed issues related to crypto-assets within banking organizations on an international basis. Finally, the FDIC has coordinated with the Board of Governors of the Federal Reserve System and the Office of the Comptroller of the Currency on supervisory matters related to crypto-asset related activities involving banking organizations.

Evidence of the FDIC's coordination with other regulators, within our jurisdiction and authorities on crypto-asset related matters, is found in recent issuances from existing coordination mechanisms, including, but not limited to:

1) FSOC Report on Digital Asset Financial Stability Risks and Regulation (issued on October 2022);[3]

2) Basel Committee's Prudential treatment of crypto-asset exposures (issued December 2022[4] following public consultations in June 2021 and July 2022);

3) FDIC, OCC, and Federal Reserve's Joint Statement on Crypto-Asset Risks to Banking Organizations (issued January 2023);[5] and,

4) various reports in response to the Executive Order on Ensuring Responsible Development of Digital Assets, in which several agencies, including the FDIC were consulted (issued throughout 2022).

We believe it is important for regulatory responses to crypto-asset related activities to be cautious and deliberate for several reasons: (a) the risk of crypto-related activities to safety and soundness, consumer protection, and financial stability; (b) the lack of history and familiarity with these assets both in the marketplace and within regulated financial institutions; and (c) the

[1] FSOC is a collaborative body chaired by the Secretary of the Treasury that brings together the expertise of the federal financial regulators, an independent insurance expert appointed by the President, and state regulators. Voting members include: the Secretary of the Treasury; the Chairman of the Board of Governors of the Federal Reserve System; the Comptroller of the Currency; the Director of the Bureau of Consumer Financial Protection; the Chairman of the Securities and Exchange Commission; the Chairperson of the Federal Deposit Insurance Corporation; the Chairperson of the Commodity Futures Trading Commission; the Director of the Federal Housing Finance Agency; the Chairman of the National Credit Union Administration; and an independent member with insurance expertise who is appointed by the President and confirmed by the Senate. Also, FSOC includes five nonvoting members.

[2] The Basel Committee on Banking Supervision (BCBS) is the primary global standard setter for the prudential regulation of banks and provides a forum for regular cooperation on banking supervisory matters. Its 45 members comprise central banks and bank supervisors from 28 jurisdictions, including the Federal Deposit Insurance Corporation, Federal Reserve, and Office of the Comptroller of the Currency.

[3] Financial Stability Oversight Council. (October 2022). Report on Digital Asset Financial Stability Risks and Regulation, available at https://home.treasury.gov/system/files/261/FSOC-Digital-Assets-Report-2022.pdf

[4] Basel Committee on Banking Supervision. (December 2022). Prudential treatment of crypto-asset exposures, available at https://www.bis.org/bcbs/publ/d545.pdf

[5] FDIC Press Release-2-23: Agencies Issue Joint Statement on Crypto-Asset Risks to Banking Organizations, January 3, 2022, available at https://www.fdic.gov/news/press-releases/2023/pr23002a.pdf

Mr. Clements, Director

dynamic nature of these assets. The FDIC's actions clearly reflect this approach to bank participation in crypto-asset related activity, of which blockchain technologies are a part.

In April 2022, the FDIC issued a Financial Institution Letter, asking FDIC-supervised banks to notify the FDIC if they are engaging in, or planning to engage in, crypto-asset related activities.[6] The FDIC requests that institutions provide information necessary to allow the agency to assess the safety and soundness, consumer protection, and financial stability implications. The FDIC is providing relevant case specific supervisory feedback to the FDIC-supervised institution, as appropriate, in a timely manner. The other federal banking agencies have issued similar requests to their supervised institutions.[7] As the FDIC and the other federal banking agencies develop a better collective understanding of the risks associated with these activities, we expect to provide broader industry guidance on an interagency basis. In summary, the FDIC plans to continue to collaborate with other regulators, where appropriate, to assess risks to the banking system posed by crypto-asset related activities, including blockchain technologies, and to respond appropriately.

Thank you for your efforts and if you have any questions or need additional follow-up information, please do not hesitate to contact Management Analyst Megan Patzwall at (703) 562-2627 or mpatzwall@fdic.gov.

Sincerely,

DOREEN EBERLEY Digitally signed by DOREEN EBERLEY Date: 2023.02.03 18:14:39 -05'00'

Doreen R. Eberley
Director

[6] FDIC Financial Institution Letter 16–2022: Notification of Engaging in Crypto–Related Activities, April 7, 2022, available at https://www.fdic.gov/news/financial-institution-letters/2022/fil22016.html

[7] 2 See OCC Interpretive Letter 1179 "Chief Counsel's Interpretation Clarifying: (1) Authority of a Bank to Engage in Certain Cryptocurrency Activities; and (2) Authority of the OCC to Charter a National Trust Bank," (November 18, 2021); and Federal Reserve SR 22-6 / CA 22-6: "Engagement in Crypto-Asset-Related Activities by Federal Reserve Supervised Banking Organizations," (August 16, 2022).

Appendix V: Comments from National Credit Union Administration

National Credit Union Administration
Office of the Executive Director

February 2, 2023

Mr. Michael Clements
Director, Financial Markets & Community Investment
U.S. Government Accountability Office
441 G Street NW
Washington, DC 20548

Dear Mr. Clements,

The National Credit Union Administration (NCUA) has reviewed the Government Accountability Office's draft report (GAO 23-4105346) entitled Blockchain in Finance – Legislative and Regulatory Actions Needed to Ensure Comprehensive Oversight of Crypto Assets. The draft report includes the following recommendation for the NCUA:

Recommendation: The Chairman of the NCUA should jointly establish with the CFPB [Consumer Financial Protection Bureau], CFTC [Commodity Futures Trading Commission], FDIC [Federal Deposit Insurance Corporation], Federal Reserve, OCC [Office of the Comptroller of the Currency], and SEC [Securities and Exchange Commission] a formal coordination mechanism for collectively identifying risks posed by blockchain-based products and services and formulating a timely regulatory response. To facilitate these objectives, this mechanism could include formal planning documents that establish the frequency of meetings and processes for identifying risks and responding to them within agreed-upon timeframes.

Response: NCUA agrees with the recommendation.

Thank you for the opportunity to review and comment on the draft report.

Sincerely,

LARRY FAZIO
Digitally signed by LARRY FAZIO
Date: 2023.02.01 13:02:55 -05'00'

Larry Fazio
Executive Director

Appendix VI: Comments from the Office of the Comptroller of the Currency

Office of the Comptroller of the Currency

Washington, DC 20219

February 3, 2023

Mr. Michael E. Clements
Director, Financial Markets and Community Investment
U. S. Government Accountability Office
Washington, DC 20548

Dear Mr. Clements:

Thank you for providing the Office of the Comptroller of the Currency (OCC) an opportunity to review the Government Accountability Office's (GAO) draft report titled *Blockchain in Finance: Legislative and Regulatory Actions Needed to Ensure Comprehensive Oversight of Crypto Assets (GAO-23-105346).* Technical edits have been provided separately.

As part of this review, the GAO has provided the following recommendation:

The Comptroller of the Currency should jointly establish with CFPB, CFTC, FDIC, Federal Reserve, NCUA, and SEC a formal coordination mechanism for collectively identifying risks posed by blockchain-based products and services and formulating a timely regulatory response. To facilitate these objectives, this mechanism could include formal planning documents that establish the frequency of meetings and processes for identifying risks and responding to them within agreed-upon timeframes.

The OCC understands that distributed ledger technology, such as Blockchain, may be beneficial to the financial sector but also have the potential to introduce significant or unexpected risks. The OCC has adopted a careful and cautious approach in this area and recognizes the importance of interagency collaboration and coordination among financial regulators to monitor opportunities and risks. Notably, Acting Comptroller of the Currency Hsu has stated "interagency and international collaboration and coordination sits at the heart of the OCC's approach to crypto,"[1] which also aligns with the OCC Strategic Plan, Fiscal Years 2023-2027.[2]

The OCC continues to monitor, separately and in collaboration with other regulatory agencies, market and financial sector adoption of distributed ledger technology. The OCC participates in broader sector collaboration through formal coordination mechanisms that exist under the authority of the Financial Stability Oversight Council (FSOC), the Financial and Banking Information Infrastructure Committee (FBIIC)[3], Financial Literacy and Education Commission

[1] Acting Comptroller of the Currency Michael J. Hsu Remarks to the Harvard Law School and Program on International Financial Systems Roundtable on Institutional Investors and Crypto Assets (occ.gov)
[2] OCC Strategic Plan, Fiscal Years 2023-2027
[3] The Committee consists of 18 member organizations from across the financial regulatory community, both federal and state.

(FLEC)[4], and the Federal Financial Institutions Examination Council (FFIEC)[5]. These existing committees and councils have established governing processes that support organized collaboration, information sharing agreements, and protocols that facilitate consensus building or actionable strategies.

As a general matter, the OCC believes the FSOC provides an effective and efficient formal coordination mechanism to support collective identification of risks posed by distributed ledger-based products and services. As a forum for discussion and analysis, FSOC supports the timely identification of emerging risks and systemic issues. As noted in its "Report on Digital Asset Financial Stability Risks and Regulations," the FSOC acknowledges the importance of coordination across regulatory agencies to ensure regulatory standards remain high and on a level playing field. Development in distributed ledger technology is dynamic and rapidly evolving. As such, the OCC suggests that regulatory coordination through FSOC, in accordance with established authorities, be flexible in purpose and agile in approach.

In addition to coordination through FSOC, as needed, other existing formal coordination mechanisms (e.g., FBIIC, FLEC and FFIEC) would be available to support collective identification of risks arising from distributed ledger-based products and services. Further, the OCC would continue to collaborate with numerous agencies across the U.S. government. Examples of collaboration include:

- Consideration of President Biden's March 9, 2022, Executive Order (EO), which outlined the first whole-of-government approach to addressing the risks and harnessing the potential benefits of digital assets and their underlying technology and developing frameworks and policy recommendations that advance key priorities.
- Collaboration with the President's Working Group on stablecoins;[6]
- Ongoing collaboration and coordination with other federal banking agencies (Federal Reserve and FDIC) to assess and identify key risks associated with crypto-assets, including a statement on January 3, 2023, highlighting key risks for banking organizations associated with crypto-assets and the crypto-asset sector and describing the agencies' approaches to supervision in this area.[7]

If you need additional information, please contact Grovetta N. Gardineer, Senior Deputy Comptroller, Bank Supervision Policy, at (202) 649-6770.

Sincerely,

G. N. Gardineer

Grovetta N. Gardineer
Senior Deputy Comptroller for Bank Supervision Policy

[4] The Commission is made up of the heads of 19 federal agencies.
[5] The Council is a formal interagency body empowered to prescribe uniform principles, standards, and report forms for the federal examination of financial institutions by the Federal Reserve, FDIC, NCUA OCC and CFPB.
[6] President's Working Group on Financial Markets Releases Report and Recommendations on Stablecoins
[7] *OCC Bulletin 2023-1, "Joint Statement on Crypto-Asset Risks to Banking Organizations."*

2

Appendix VII: Comments from Securities and Exchange Commission

UNITED STATES
SECURITIES AND EXCHANGE COMMISSION
WASHINGTON, D.C. 20549

May 2, 2023

Michael E. Clements
Director, Financial Markets and Community Investment
U.S. Government Accountability Office
441 G Street, NW
Washington, DC 20548

Dear Mr. Clements:

Thank you for sending the GAO's draft report, *Blockchain in Finance: Legislative and Regulatory Actions Needed to Ensure Comprehensive Oversight of Crypto Assets* (GAO-23-105346). We appreciate the opportunity to review the GAO's proposed findings related to the regulation of blockchain-based financial products and services.

While we appreciate the GAO's undertaking to review federal oversight of crypto assets, the terminology, descriptions, and findings related to crypto assets and to the crypto asset industry generally, as currently set forth in the draft report, are those of the GAO, and they do not reflect the views of the SEC on these issues, nor does the SEC agree with all of the draft report's apparent positions regarding the crypto asset industry's risks and the applicability of the federal securities laws to various aspects of the crypto asset industry. Nevertheless, we are encouraged to see that the report's proposed findings underscore the importance of the SEC's role in safeguarding market integrity and financial stability, and protecting retail investors, from the many risks caused by crypto asset securities platforms and other industry participants acting in non-compliance with existing securities laws and regulations. The SEC remains committed to our mission of protecting investors, maintaining fair, orderly, and efficient markets, and facilitating capital formation.

The draft GAO report recommends that the SEC and other regulators establish "a formal coordination mechanism for collectively identifying risks posed by blockchain-based products and services and formulating a timely regulatory response." We believe that our extensive longstanding and ongoing efforts to coordinate within the U.S. Government (including with the CFPB, CFTC, FDIC, Federal Reserve Board, NCUA, and OCC), through, for example, the Financial Stability Oversight Council (FSOC), the President's Working Group on Financial Markets (PWG), the Financial Literacy and Education Commission (FLEC), joint participation in international bodies, and other bi-lateral and multi-lateral efforts, have protected investors and the U.S. economy more broadly.

Thank you for the consideration you and your staff have shown our agency during this engagement. If you have any questions, please do not hesitate to contact me at (202) 551-4306.

Sincerely,

KENNETH JOHNSON
Digitally signed by KENNETH JOHNSON
Date: 2023.05.02 15:26:56 -04'00'

Kenneth A. Johnson
Chief Operating Officer

Appendix VIII: GAO Contact and Staff Acknowledgments

GAO Contact

Michael E. Clements, (202) 512-8678 or clementsm@gao.gov

Staff Acknowledgments

In addition to the contact named above, Stefanie Jonkman (Assistant Director), Chris Ross (Analyst in Charge), Andrew Altobello, Rachel DeMarcus, Dan Luo, Jason Marshall, Alicia Martinez, Marc Molino, Barbara Roesmann, and Farrah Stone made key contributions to this report.

GAO's Mission

The Government Accountability Office, the audit, evaluation, and investigative arm of Congress, exists to support Congress in meeting its constitutional responsibilities and to help improve the performance and accountability of the federal government for the American people. GAO examines the use of public funds; evaluates federal programs and policies; and provides analyses, recommendations, and other assistance to help Congress make informed oversight, policy, and funding decisions. GAO's commitment to good government is reflected in its core values of accountability, integrity, and reliability.

Obtaining Copies of GAO Reports and Testimony

The fastest and easiest way to obtain copies of GAO documents at no cost is through our website. Each weekday afternoon, GAO posts on its website newly released reports, testimony, and correspondence. You can also subscribe to GAO's email updates to receive notification of newly posted products.

Order by Phone

The price of each GAO publication reflects GAO's actual cost of production and distribution and depends on the number of pages in the publication and whether the publication is printed in color or black and white. Pricing and ordering information is posted on GAO's website, https://www.gao.gov/ordering.htm.

Place orders by calling (202) 512-6000, toll free (866) 801-7077, or TDD (202) 512-2537.

Orders may be paid for using American Express, Discover Card, MasterCard, Visa, check, or money order. Call for additional information.

Connect with GAO

Connect with GAO on Facebook, Flickr, Twitter, and YouTube.
Subscribe to our RSS Feeds or Email Updates. Listen to our Podcasts.
Visit GAO on the web at https://www.gao.gov.

To Report Fraud, Waste, and Abuse in Federal Programs

Contact FraudNet:

Website: https://www.gao.gov/about/what-gao-does/fraudnet

Automated answering system: (800) 424-5454 or (202) 512-7700

Congressional Relations

A. Nicole Clowers, Managing Director, ClowersA@gao.gov, (202) 512-4400, U.S. Government Accountability Office, 441 G Street NW, Room 7125, Washington, DC 20548

Public Affairs

Chuck Young, Managing Director, youngc1@gao.gov, (202) 512-4800
U.S. Government Accountability Office, 441 G Street NW, Room 7149
Washington, DC 20548

Strategic Planning and External Liaison

Stephen J. Sanford, Managing Director, spel@gao.gov, (202) 512-4707
U.S. Government Accountability Office, 441 G Street NW, Room 7814, Washington, DC 20548