STRENGTHENING AMERICAN

Contents

Acronyms and Abbreviations

ACH Automated Clearing House Advisers Act Investment Advisers Act of 1940 AEC Anonymity-Enhanced Cryptocurrency AFSI Adjusted Financial Statement Income AICPA American Institute of Certified Public Accountants

AML Anti-Money Laundering

AML Act Anti-Money Laundering Act of 2020 API Application Programming Interface ASIC Application-Specific Integrated Circuit ATIF Automated Threat Information Feed ATS Alternative Trading System BCBS Basel Committee on Banking Supervision

BHC Bank Holding Company

BSA Bank Secrecy Act

CAMT Corporate Alternative Minimum Tax CARF Crypto-Asset Reporting Framework CBDC Central Bank Digital Currency CCP Central Counterparty

CCULR Complex Credit Union Leverage Ratio CEA Commodity Exchange Act CEX Centralized Digital Asset Exchange CFT Countering the Financing of Terrorism CFPB Consumer Financial Protection Bureau

CFTC Commodity Futures Trading Commission

CIP Customer Identification Program CLARITY Digital Asset Market Clarity Act of 2025 CSD Central Securities Depository CTA Commodity Trading Advisor CUSO Credit Union Service Organization CVC Convertible Virtual Currency DAMS CFTC GMAC Digital Asset Markets Subcommittee

DAO Decentralized Autonomous Organization dApp Decentralized Application DCM Designated Contract Markets DCO Derivatives Clearing Organization DeFi Decentralized Finance

DePIN Decentralized Physical Infrastructure DEX Decentralized Exchange

DIF Deposit Insurance Fund

DLT Distributed Ledger Technology

DOJ U. S. Department of Justice DPRK Democratic People's Republic of Korea ECB European Central Bank

ECP Eligible Contract Participant ETF Exchange-Traded Fund

ETN Exchange-Traded Note

ETP Exchange-Traded Product EU European Union

Exchange Act Securities Exchange Act of 1934 FASB Financial Accounting Standards Board FATCA Foreign Account Tax Compliance Act FATF Financial Action Task Force FBAR Report of Foreign Bank and Financial Accounts

FBI Federal Bureau of Investigation FBIIC Financial and Banking Information Infrastructure Committee

FCM Futures Commission Merchant FCUA Federal Credit Union Act

FDIC Federal Deposit Insurance Corporation FHFA Federal Housing Finance Agency FHC Financial Holding Company FinCEN Financial Crimes Enforcement Network FINRA Financial Industry Regulatory Authority

FIPS Federal Information Processing Standards

FMI Financial Market Infrastructure FRB Board of Governors of the Federal Reserve System

FRS Federal Reserve System

FSA Federal Savings Association FSB Financial Stability Board

FSOC Financial Stability Oversight Council FX Foreign Exchange

GAAP Generally Accepted Accounting Principles

GENIUS Guiding and Establishing National Innovation for U.S. Stablecoins Act

GMAC CFTC Global Markets Advisory Committee

HQLA High-Quality Liquid Assets IB Introducing Broker

ICO Initial Coin Offering

IEC International Electrotechnical Commission

IEEE Institute of Electrical and Electronics Engineers

IEEPA International Emergency Economic Powers Act

IIJA Infrastructure Investment and Jobs Act Investment Company Act Investment Company Act of 1940

IRS Internal Revenue Service

ISO International Organization for Standardization

IVAN Illicit Virtual Asset Notification JCT Joint Committee on Taxation LICU Low-Income Credit Union MEV Maximum Extractable Value MFA Multifactor Authentication MiCA Markets in Crypto-Assets MSB Money Services Business

NAIC National Association of Insurance Commissioners

NBA National Bank Act

NCUA National Credit Union Administration NFA National Futures Association NFT Non-Fungible Token

NIST National Institute for Standards and Technology

NMS National Market System

NSPA National Stolen Property Act NYDFS New York State Department of Financial Services

OCC Office of the Comptroller of the Currency

OCCIP Office of Cybersecurity and Critical Infrastructure Protection

OFAC Office of Foreign Assets Control OTC Over-the-Counter

P2P Peer-to-Peer

PCAOB Public Company Accounting Oversight Board

PoS Proof-of-Stake

PoW Proof-of-Work

PQC Post-Quantum Cryptography RBC Risk Based Capital

RFI Request for Information

RPC Remote Procedure Call

SAB SEC Staff Accounting Bulletin SAFT Simple Agreement for Future Tokens SAR Suspicious Activity Report SDO Standards Development Organization SEC Securities and Exchange Commission Securities Act Securities Act of 1933

SEF Swap Execution Facility

SIPA Securities Investor Protection Act of 1970 SMS Short Message Service

SRO Self-Regulatory Organization SWIFT Society for Worldwide Interbank Financial Telecommunication

TradFi Traditional Finance

Treasury U.S. Department of the Treasury TVL Total Value Locked

TWEA Trading with the Enemy Act of 1917 UK United Kingdom

VASP Virtual Asset Service Provider W3C World Wide Web Consortium Working Group President's Working Group on Digital Asset Markets

STRENGTHENING AMERICAN LEADERSHIP IN DIGITAL FINANCIAL TECHNOLOGY [1]

Executive Order 14178 of January 23, 2025

The digital asset industry plays a crucial role in innovation and economic development in the United States, as well as our Nation's international leadership. It is therefore the policy of my Administration to support the responsible growth and use of digital assets, blockchain technology, and related technologies across all sectors of the economy, including by:

(i) protecting and promoting the ability of individual citizens and private-sector entities alike to access and use for lawful purposes open public blockchain networks without persecution, including the ability to develop and deploy software, to participate in mining and validating, to transact with other persons without unlawful censorship, and to maintain self-custody of digital assets;

(ii) promoting and protecting the sovereignty of the United States dollar, including through actions to promote the development and growth of lawful and legitimate dollar-backed stablecoins worldwide;

(iii) protecting and promoting fair and open access to banking services for all law-abiding individual citizens and private-sector entities alike;

(iv) providing regulatory clarity and certainty built on technology-neutral regulations, frameworks that account for emerging technologies, transparent decision making, and well-defined jurisdictional regulatory boundaries, all of which are essential to supporting a vibrant and inclusive digital economy and innovation in digital assets, permissionless blockchains, and distributed ledger technologies; and

(v) taking measures to protect Americans from the risks of Central Bank Digital Currencies (CBDCs), which threaten the stability of the financial system, individual privacy, and the sovereignty of the United States, including by prohibiting the establishment, issuance, circulation, and use of a CBDC within the jurisdiction of the United States.

There is hereby established within the National Economic Council the President's Working Group on Digital Asset Markets (Working Group). The Working Group shall be chaired by the Special Advisor for AI and Crypto (Chair).

Within 180 days of the date of this order, the Working Group shall submit a report to the President, through the Assistant to the President for National Economic Policy, which shall recommend regulatory and legislative proposals that advance the policies established in this order.

DONALD J. TRUMP

PRESIDENT OF THE UNITED STATES

1 Exec. Order No. 14178, Strengthening American Leadership in Digital Financial Technology, 90 Fed. Reg. 8647 §§ 1, 4 (Jan. 31, 2025). Executive Order excerpted for brevity.

MEMBERS OF THE WORKING GROUP[2]

Chair David Sacks, Special Advisor for AI and Crypto

Scott Bessent, Secretary of the Treasury

Pam Bondi, Attorney General

Howard Lutnick, Secretary of Commerce

Kristi Noem, Secretary of Homeland Security

Russell Vought, Director of the Office of Management and Budget

Marco Rubio, Acting Assistant to the President for National Security Affairs

Robin Colwell, Deputy Assistant to the President for National Economic Policy

Stephen Miller, Homeland Security Advisor

Paul Atkins, Chairman of the Securities and Exchange Commission

Caroline Pham, Acting Chairman of the Commodity Futures Trading Commission

Robert "Bo" Hines, Executive Director of the Working Group

2 Exec. Order No. 14178, *supra* note 1, at § 4(a) establishes the President's Working Group on Digital Asset Markets, which is chaired by the Special Advisor for AI and Crypto and includes the following officials, or their designees: the Secretary of the Treasury, the Attorney General, the Secretary of Commerce, the Secretary of Homeland Security, the Director of the Office of Management and Budget, the Assistant to the President for National Security Affairs, the Assistant to the President for National Economic Policy, the Assistant to the President for Science and Technology, the Homeland Security Advisor, the Chairman of the Securities and Exchange Commission, and the Chairman of the Commodity Futures Trading Commission. The Working Group, while

formulating its recommendations, also consulted with the Board of Governors of the Federal Reserve System, the Office of the Comptroller of the Currency, the Federal Deposit Insurance Corporation, and the National Credit Union Administration, and their designees.

Staff Acknowledgments

The Working Group would like to thank the staff of each department and agency for their contributions to this report. Specifically, the Working Group would like to thank the following:

Tyler Williams, Andrew Rittenhouse, Thomas Weidner, Jonathan Hurowitz, and Frank Sensenbrenner from the Department of the Treasury; Chris DeLorenz from the Department of Justice; Patrick Butler, Dylan Clement, and Chris Netram from the Department of Commerce; Joseph Alm from the Department of Homeland Security; Dr. Mark Calabria from the Office of Management and Budget; Jeff Wrase from the National Economic Council; Emily Underwood, Special Assistant to the President and Policy Advisor; Taylor Asher, Michael Selig, and Philip Raimondi from the Securities and Exchange Commission; and Harry Jung, Meghan Tente, and Brigitte Weyls from the Commodity Futures Trading Commission.

I. Introduction

CHAPTER I

Introduction

Introduction

The American story is one of innovation. From the railroads that linked sea to shining sea, to the internet that connected the entire world, American entrepreneurs have led the buildout of next generation technologies in every generation since our founding. Crypto[3] should be no different.

The Working Group, as the author of this report, endorses the notion that digital assets and blockchain technologies can revolutionize not just America's financial system, but systems of ownership and governance economy-wide. American entrepreneurs who pioneer new industries using these technologies deserve both clarity on the policies that affect their efforts and praise for the progress they have made. The Working Group further believes that the movement underpinning crypto's development—largely grassroots and dedicated to building a more open and efficient financial system for all—should be recognized. No President gave this movement the recognition it deserves until President Trump.

As of June 2025, President Trump's approval rating among investors in cryptocurrencies was 72%.[4] For context, private surveys suggestthat more than one in five Americans, or over 68 million people, own cryptocurrencies.[5] 82% ofthese investors believed June 2025 to be a good time to investin cryptocurrencies,[6] and 64% said President Trump's policies made them more likely to do so.[7] The optimism extended to institutional investors too; 83% planned to increase their allocations to digital assets in 2025 per a survey conducted after the election.[8] The first quarter of 2025 saw venture capitalists deploy $4.8 billion into crypto and blockchain-focused startups,[9] supporting industry forecasts of a 70% year-over-year increase in total venture dollars invested.[10]

The difference from prior years is stark. The Biden Administration's approach to crypto was marked by

regulatory overreach[11] that countered the American tradition of embracing new technologies. Operation Choke Point 2.0[12] saw regulators push banks to cut off lawful crypto businesses, effectively debanking the industry.[13] This aggressive strategy of regulation by enforcement created a hostile environment for crypto entrepreneurs[14]

3 In this report, the term "crypto" is used to describe the ecosystem and technologies built around digital assets and blockchains, including the users, developers, businesses, and enthusiasts engaged in these domains.

4 *HarrisX Crypto Policy Study June 2025*, HarrisX, https://www.harrisx.com/posts/crypto-policy-june-25 (last visited July 13, 2025). 5 National Cryptocurrency Association, 2025 State of Crypto Holders Report (Apr. 2, 2025), https://nca.org/report.pdf; *2025 Cryptocurrency Adoption and Consumer Sentiment Report*, Security.Org, https://www.security.org/digital-security/cryptocurrency-annual-consumer-report (last updated Jan. 31, 2025); *Introducing the 2025 Global State of Crypto Report*, Gemini (May 27, 2025), https://www.gemini.com/blog/introducing-the-2025-global-state-of-crypto-report. 6 HarrisX, *supra* note 4.

7 *Id.*

8 Prashant Kher & Scott Mickey, *Growing Enthusiasm Propels Digital Assets into the Mainstream,* EY Parthenon (Mar. 18, 2025), https://www.ey.com/en_us/insights/financial-services/growing-enthusiasm-and-adoption-of-digital-assets.

9 Alex Thorn, *Crypto & Blockchain Venture Capital - Q1 2025*, Galaxy (May 1, 2025), https://www.galaxy.com/insights/research/crypto-venture-capital-q1-2025.

10 Leah Hodgson, *Sygnum Rides VC Crypto Wave to Unicorn Status*, PitchBook (Jan. 14, 2025), https://pitchbook.com/news/articles/sygnum-rides-vc-crypto wave-to-unicorn-status.

11 *See, e.g., Crypto Freedom All. of Tex. v. SEC*, No. 24-cv-361 (N.D. Tex. Nov. 21, 2024) (vacating the SEC's rulemaking to expand the definition of the term "dealer" for exceeding the SEC's statutory authority).

12 *See generally* Hearing on *Operation Choke Point 2.0: The Biden Administration's Efforts to Put Crypto in the Crosshairs*, Before the H. Comm. on Fin. Servs., 119th Cong. (2025).

13 See, e.g., David H. Thompson et al., *Operation Choke Point 2.0: The Federal Bank Regulators Come For Crypto,* Cooper & Kirk (Mar. 24, 2023), https://www.cooperkirk.com/wp-content/uploads/2023/03/Operation-Choke-Point-2.0.pdf; *The Debanking of the Crypto Industry: Examining the Role of the FDIC*, Hearing Before the Subcomm. On Oversight & Investigations of the H. Comm. On Fin. Servs., 119th Cong. (Feb. 6, 2025) (statement of Paul Grewal, Chief Legal Officer, Coinbase), https://www.congress.gov/119/meeting/house/117858/witnesses/HHRG-119-BA09-Wstate-GrewalP-20250206.pdf.

14 *See, e.g.,* Commissioners Hester M. Peirce & Mark T. Uyeda, U.S. Securities and Exchange Commission (SEC), *Omakase: Statement on In the Matter of Flyfish Club, LLC* (Sept. 16, 2024), https://www.sec.gov/newsroom/speeches-statements/peirce-uyeda-statement-flyfish-091624 (stating that addressing crypto "in an endless series of misguided and overreaching cases has been and continues to be a consequential mistake"); Commissioners Hester M. Peirce & Mark T. Uyeda, SEC, *On Today's Episode of As the Crypto World Turns: Statement on ShapeShift AG* (Mar. 5, 2024), https://www.sec.gov/newsroom/speeches statements/peirce-uyeda-statement-crypto-world-turns-03-06-24 (stating that the SEC's enforcement action "adds to the ambiguity that hangs over the crypto world"); Commissioners Hester M. Peirce & Mark T. Uyeda, SEC, *Collecting Enforcement Actions: Statement on Stoner Cats 2, LLC* (Sept. 13, 2023), https://www.sec.gov/newsroom/speeches-statements/peirce-uyeda-statement-stonercats-091323 (stating that the SEC's analysis of non-fungible tokens lacked "any meaningful limiting principle. It carries implications for creators of all kinds. Were we to apply the securities laws to physical collectibles in the same way we apply them to NFTs, artists' creativity would wither in the shadow of legal ambiguity.").

that at times drove their projects and ventures overseas. Although a great deal of the early innovation in the crypto space occurred in the United States, much of the industry's corporate infrastructure migrated offshore to avoid the unfavorable regulatory environment. This approach nearly eliminated the opportunity for the United States to lead in this revolutionary technology due to mere political whims.

President Trump's election marked an end to this misstep. It was America's hard fork—the end of one chain of poor policy decisions in favor of an updated, better approach. The Working Group encourages the Federal government to operationalize President Trump's promise to make America the "crypto capital of the world"[15] and adopt a pro-innovation mindset toward digital assets and blockchain technologies. The following core recommendations, if implemented, will ensure crypto becomes a hallmark of the new American Golden Age.

American citizens and businesses should be able to own digital assets and use blockchain technologies for lawful purposes without fear of prosecution. Likewise, American entrepreneurs and software developers should have the liberty, and regulatory certainty, to upgrade all sectors of our economy using these technologies.

- Congress should enact legislation affirming that individuals can custody their own digital assets without a financial intermediary and engage in lawful peer-to-peer transactions using those assets. • Congress should codify principles regarding how control over an asset impacts Bank Secrecy Act (BSA) obligations, particularly for money transmitters. A software provider that does not maintain total independent control over value should not be considered as engaged in money transmission for purposes of the BSA.
- The Financial Crimes Enforcement Network (FinCEN) should evaluate whether and how its existing guidance related to the digital asset sector, including the guidance issued in 2013 and 2019, should be rescinded, modified, or updated to reflect legislative and regulatory changes. As part of this effort, FinCEN could consider whether additional guidance would be helpful for particular market segments or

for application of particular BSA obligations.

Policymakers and market regulators should lay the groundwork for American digital asset markets to become the deepest and most liquid in the world.

- The Securities and Exchange Commission and the Commodity Futures Trading Commission should use their existing authorities to immediately enable the trading of digital assets at the Federal level. • Congress should enact legislation that grants the Commodity Futures Trading Commission clear authority to regulate spot markets in non-security digital assets. This legislation should permit both market regulators' registrants to engage in multiple business lines under the most efficient licensing structure possible.
- Policymakers should embrace decentralized finance as an option for individuals and investors and appreciate the extent to which a given software application: (i) exercises "control" over assets; (ii) is technologically capable of being modified; (iii) operates with a centralized structure or management; and (iv) is logistically capable of complying with current regulatory obligations when determining its regulatory treatment.

15 *Issues: Technology & Innovation*, The White House, https://www.whitehouse.gov/issues/tech-innovation (last visited July 13, 2025).

Banking regulators should never again pursue the Biden Administration's policies of Operation Choke Point 2.0 and should instead embrace the opportunities digital assets and blockchain technologies offer to banks nationwide.

- Federal banking regulators should ensure that existing and new best practices or guidance on risk management and bank engagement are technology-neutral and that expectations regarding offering banking services do not discriminate against lawful businesses solely due to their industry.
- These regulators should relaunch crypto innovation efforts to provide clarity on the activities that banks want to pursue, with a clear process for considering additional activities. To support these efforts, the United States should adopt capital requirements for bank digital asset activities that accurately reflect the risk of the asset or activity.
- The relevant Federal banking regulators should provide clarity and transparency regarding the process for eligible institutions to obtain a bank charter or a Reserve Bank master account.

U.S. dollar-backed stablecoins represent the next wave of innovation in payments, and policymakers should encourage their adoption to advance U.S. dollar dominance in the digital age.

- All agencies to which Congress delegated responsibilities under the GENIUS Act should faithfully and expeditiously execute those responsibilities.
- Relevant U.S. agencies, including Treasury, should promote U.S. private sector leadership in the responsible development of cross-border payments and financial markets technologies. These agencies should also promote U.S. leadership in establishing international legal, regulatory, and technical standards and best practices for new payments technologies that reflect U.S. interests and values.
- Congress should enact legislation prohibiting the adoption of any CBDCs in the United States. Internationally, the United States should urge other countries to adopt policies that promote the role of the

private sector in upgrading payments and financial systems.

U.S. law enforcement agencies should have the tools and authorities to hold those who use digital assets for illegal activities accountable. These tools should never be misused to target the lawful activities of law-abiding citizens.

- Congress should consider clarifying language regarding the BSA's application to foreign-located actors, taking into consideration the extent to which a foreign-located actor's conduct, and the effect of such conduct on the United States, warrants reach of U.S. law.
- Treasury should undertake efforts to encourage greater information sharing between the private and public sectors to more effectively target bad actors operating in the digital asset ecosystem. This information sharing must only be used for the purpose prescribed in law of targeting illicit finance and terrorist activity.
- Treasury and the agencies to which it has delegated responsibility for AML/CFT examinations should identify areas of uncertainty for traditional financial institutions providing services to digital asset actors and digital asset services to customers. Agencies, including Treasury and the Federal banking agencies, should provide needed guidance or other materials to help clarify AML/CFT obligations and expectations with regards to those actors and services.

Federal tax policy should recognize the unique characteristics of digital assets and address longstanding requests for guidance from investors and entrepreneurs.

- Treasury and the IRS should publish guidance on several topics, including the determination of "adjusted financial statement income" with respect to financial accounting unrealized gains and losses on investment assets other than stock and partnership interests, whether wrapping and unwrapping transactions are taxable transactions, and de minimis receipts of digital assets.
- Treasury and the IRS should review previously issued guidance related to the timing of income from staking and mining and consider whether to clarify, modify, or reverse that guidance.
- Congress should enact legislation that: (i) adds digital assets to the list of assets subject to wash sale rules; (ii) amends Section 1058 to provide that it applies to loans of actively traded fungible digital assets; and (iii) treats digital assets as a new class of assets subject to modified versions of tax rules applicable to securities or commodities for federal income tax purposes.

All recommendations, and further details on the above, can be found throughout the report. Much of the discussion leading up to the recommendations assumes a baseline understanding of crypto and its novel characteristics. The following box provides an overview, focusing particularly on the blockchain technology at its foundation.

Crypto 101

> Writing a description forthis thing for general audiences is bloody hard. There's nothing to relate it to.
>
> BitcoinTalk Forum Post Re: "Slashdot Submission for 1.0"
> Satoshi Nakamoto, July 2010[16]

The broader ecosystem of crypto derives its name from cryptocurrencies—digital currencies that can be transferred peer-to-peer over the internet. Satoshi Nakamoto, a pseudonymous developer active in the wake of the 2008 financial crisis, created Bitcoin,[17] the first cryptocurrency, using a pioneering concept known as distributed ledger technology (DLT).[18]

Bitcoin's implementation of DLT solved the double-spending problem that earlier attempts at digital cash tried to address.[19] If Satoshi wanted to send $10 to Hal online, there had to be some authoritative way to debit $10 from Satoshi's account and credit $10 to Hal's. Traditionally, that would be a centralized, trusted intermediary (e.g., a bank) who controlled the ledger of both accounts.

To eliminate the need for a centralized intermediary, and make the system both decentralized and

permissionless, the Bitcoin network accomplished the following:

1. Distributed the ledger among all participants in the network—meaning, each transaction would be recorded publicly with other transactions occurring around the same time in a list of transactions called a block.
2. Incentivized nodes, computers running access to the network, to solve a difficult math problem required to mine, or produce, a valid block through transaction fees and rewards.
3. Required other nodes in the network to validate the miner's work by checking the proposed block to ensure: (i) no double-spending transactions occurred, (ii) the sender of each transaction cryptographically proved the sender's ownership of the funds being sent, and (iii) the miner's solution to the math problem was correct.

If each node in the network confirmed that the proposed block passed these checks, it would be added to each node's copy of the distributed ledger as an update to the account balances—the act of reaching consensus.[20] As more blocks were created and accepted, the ledger would become a chain of blocks recording the full sequential transaction history—hence, a blockchain.

The account numbers on a blockchain are known as addresses. Anyone can create a new address to send and receive cryptocurrencies. A user first creates a private key, effectively a password, that provides the holder the ability to digitally sign transactions. This private key has a paired public key, which is used to create the address. An important feature of these key pairs is that a private key can

16 satoshi, Comment to *Re: Slashdot Submission for 1.0*, BitcoinTalk (July 5, 2010, at 9:31 PM), https://bitcointalk.org/index.php?topic=234.msg1976#msg1976. 17 As a general note, throughout this report there are references to "Bitcoin" and "bitcoin." When "Bitcoin" is capitalized, the Working Group refers to the Bitcoin network; when "bitcoin" is not capitalized, the Working Group refers to the unit used for transactions.

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

19 Esin Syonmez, *What Is Double Spending: The Problem and How Blockchain Prevents It*, Morpher (Jan. 31, 2025), https://www.morpher.com/blog/double spending.

20 Consensus is the process by which all the participants in a blockchain network (e.g., Bitcoin) agree to the at-time state of the blockchain. This ensures (i) that all nodes have the same version of the ledger, and (ii) the integrity and security of the blockchain. *See* Kraken Learn Team, *What Is a Blockchain Consensus Mechanism*, Kraken (Feb. 4, 2025), https://www.kraken.com/learn/what-is-blockchain-consensus-mechanism.

create a public key, but it is computationally intractable for conventional computers to use a public key to derive its private key.[21] This stems from a feature of the underlying math, which allows the private key to "unlock" the public key, but not the other way around.

Anyone with access to a private key can move the cryptocurrencies associated with its corresponding address. As such, digital asset custody is focused primarily on protecting private keys from being leaked, hacked, or lost. To facilitate storage of private keys, developers created different types of wallets. Software wallets hold private keys in a password-protected encrypted file and provide capabilities for users to sign transactions. Hardware wallets include a software package on a dedicated hardware device used only for storing keys and sending transactions to a blockchain. These wallets can be hot, meaning they operate on a live device connected to the internet; warm, meaning they maintain partial or selective internet connectivity; or cold, meaning they have no internet connection.

21 See *Chapter II, Cryptocurrency and the Technical Standards Landscape* for a further discussion of how quantum technology may impact the security of blockchain networks.

Software Wallets vs. Hardware Wallets[22]

Since the creation of Bitcoin's peer-to-peer payments system, the number of projects expanding the scope of these technologies has dramatically expanded. Entirely new blockchain networks, like Ethereum and Solana, support smart contracts—self-executing programs that automatically enforce agreements between users. Stablecoins, a special type of token[23] designed to maintain a stable value relative to a reference asset like the U.S. dollar, often rely on smart contracts for different aspects of their functionality.

22 Graphic prepared by Consensys.

23 "A token represents an asset issued on an existing blockchain; the transfer of tokens and the addresses that currently hold them are the subject of the network's consensus activities." *A Blockchain Glossary for Beginners: Definitions of Crypto and Web3 Terminology*, Consensys, https://consensys.io/knowledge-base/a-blockchain-glossary-for-beginners#token (last visited July 13, 2025).

Oracles connect external data sources to blockchain networks. This enables smart contracts to

execute onchain agreements based on real world prices and events. Smart contracts make decentralized applications (dApps) possible as tools for trading, lending, earning rewards, and other activities. Some dApps serve as cross-chain bridges, which transfer assets or data across blockchain networks. Assets that exist on one chain and pass through a cross-chain bridge to be represented on another are referred to as wrapped, and the ecosystem that operates around dApps is broadly known as decentralized finance (DeFi).

Some traditional finance (TradFi) institutions have explored using smart contracts to power new financial products or streamline agreements with counterparties.[24] They often build these products on permissioned blockchains, which allow an administrator to control or reverse parts of onchain transactions.[25]

Blockchain Oracles[26]

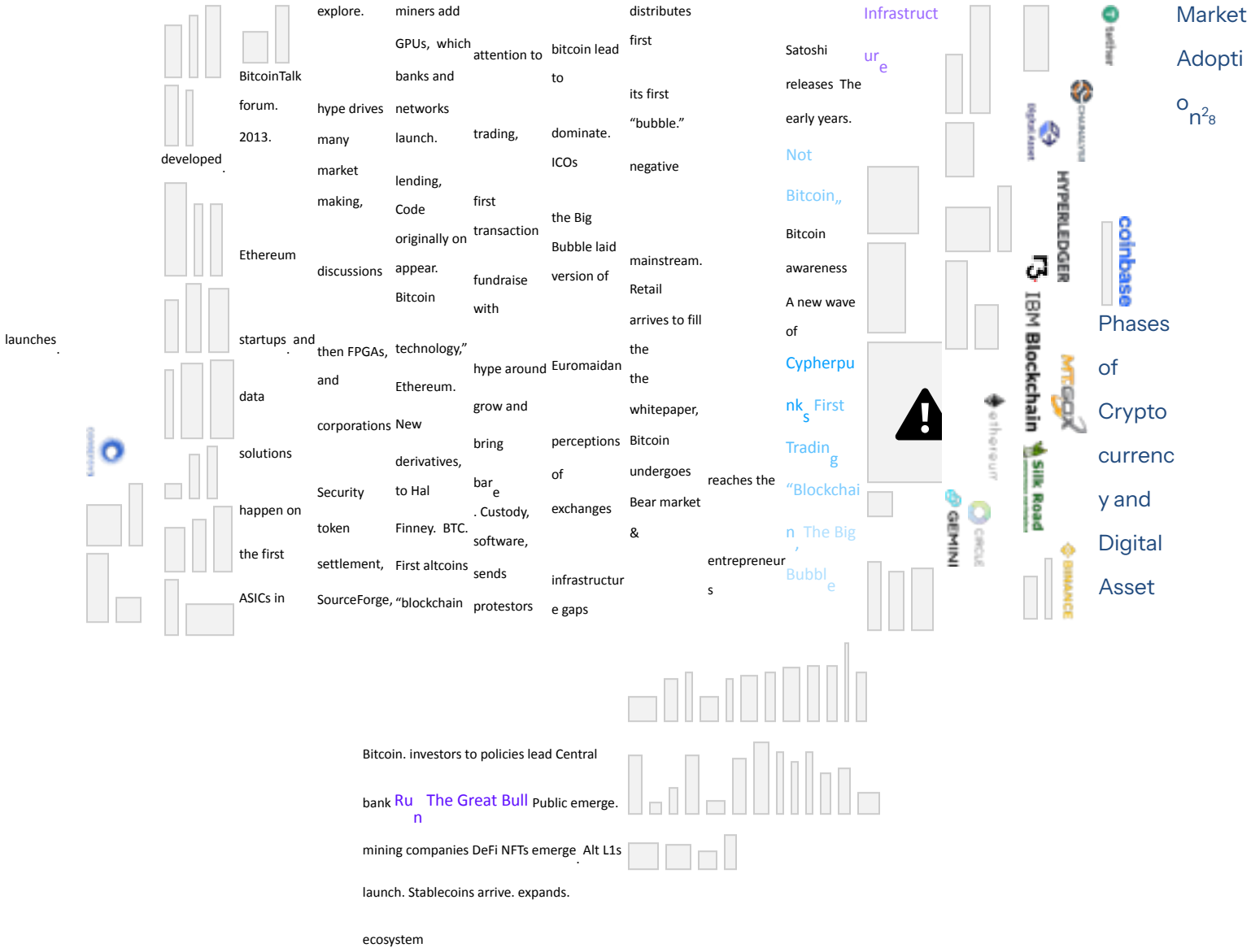
It is important to acknowledge that blockchain technology, and the opportunities it provides, did not emerge from TradFi or Washington, D.C. think tanks. Conversations on open internet forums and mailing lists[27] were the launchpads for figures like Satoshi Nakamoto to outline and debate core principles for a new, decentralized system of trust. Throughout the report, there are references to original posts to anchor the topics discussed.

24 Press Release, Citigroup Inc., Citi Develops New Digital Asset Capabilities for Institutional Clients (Sept. 18, 2023), https://www.citigroup.com/global/news/press-release/2023/citi-develops-new-digital-asset-capabilities-for-institutional-clients; *see Franklin OnChain U.S. Government Money Fund,* Franklin Templeton, https://www.franklintempleton.com/investments/options/money-market-funds/products/29386/SINGLCLASS/franklin-on-chain-u-s-government money-fund/FOBXX (last visited July 13, 2025).

25 Graeme Moore, *The Future of Tokenization? Permissioned Blockchain*s, Blockworks (May 6, 2024), https://blockworks.co/news/future-tokenization permissioned-blockchains.

26 Graphic prepared by Chainlink.

27 The *Cypherpunk mailing list* was an influential pre-Bitcoin online forum where cryptographers and privacy enthusiasts discussed ideas around digital cash, decentralization, use cases for public key cryptography. It was on this list that Satoshi Nakamoto first shared the Bitcoin whitepaper in 2008. Satoshi Nakamoto publicly announced Bitcoin on the *P2P Foundation* forum in 2009, before creating *BitcoinTalk*—a central hub for discussions around developing and debugging Bitcoin and a convening ground for the growing Bitcoin community. *See generally* Satoshi Nakamoto, *Bitcoin P2P E-Cash Paper*, Satoshi Nakamoto Institute (Oct. 31, 2008), https://satoshi.nakamotoinstitute.org/emails/cryptography/1; Satoshi Nakamoto, *Bitcoin Open Source Implementation of P2P Currency*, Satoshi Nakamoto Institute (Feb. 11, 2009), https://satoshi.nakamotoinstitute.org/posts/p2pfoundation/1; *BitcoinTalk Forum*, https://bitcointalk. org (last visited, July 13, 2025).



adoption grows .

II. The Digital Asset Ecosystem

CHAPTER II

The Digital Asset Ecosystem

The Digital Asset Ecosystem

> A purely peer-to-peer version of electronic cash would allow online payments to be sent directly from one party to another without going through a financial institution. Digital signatures provide part of the solution, but the main benefits are lost if a trusted third party is still required to prevent double-spending. We propose a solution to the double-spending problem using a peer-to-peer network. The network timestamps transactions by hashing them into an ongoing chain of hash-based proof-of-work, forming a record that cannot be changed without redoing the proof-of-work. The longest chain not only serves as proof of the sequence of events witnessed, but proof that it came from the largest pool of CPU power. As long as a majority of CPU power is controlled by nodes that are not cooperating to attack the network, they'll generate the longest chain and outpace attackers. The network itself requires minimal structure. Messages are broadcast on a best effort basis, and nodes can leave and rejoin the network at will, accepting the longest proof-of-work chain as proof of what happened while they were gone.
>
> Abstract from *Bitcoin: A Peer-to-Peer Electronic Cash System*
> Satoshi Nakamoto, October 2008[29]

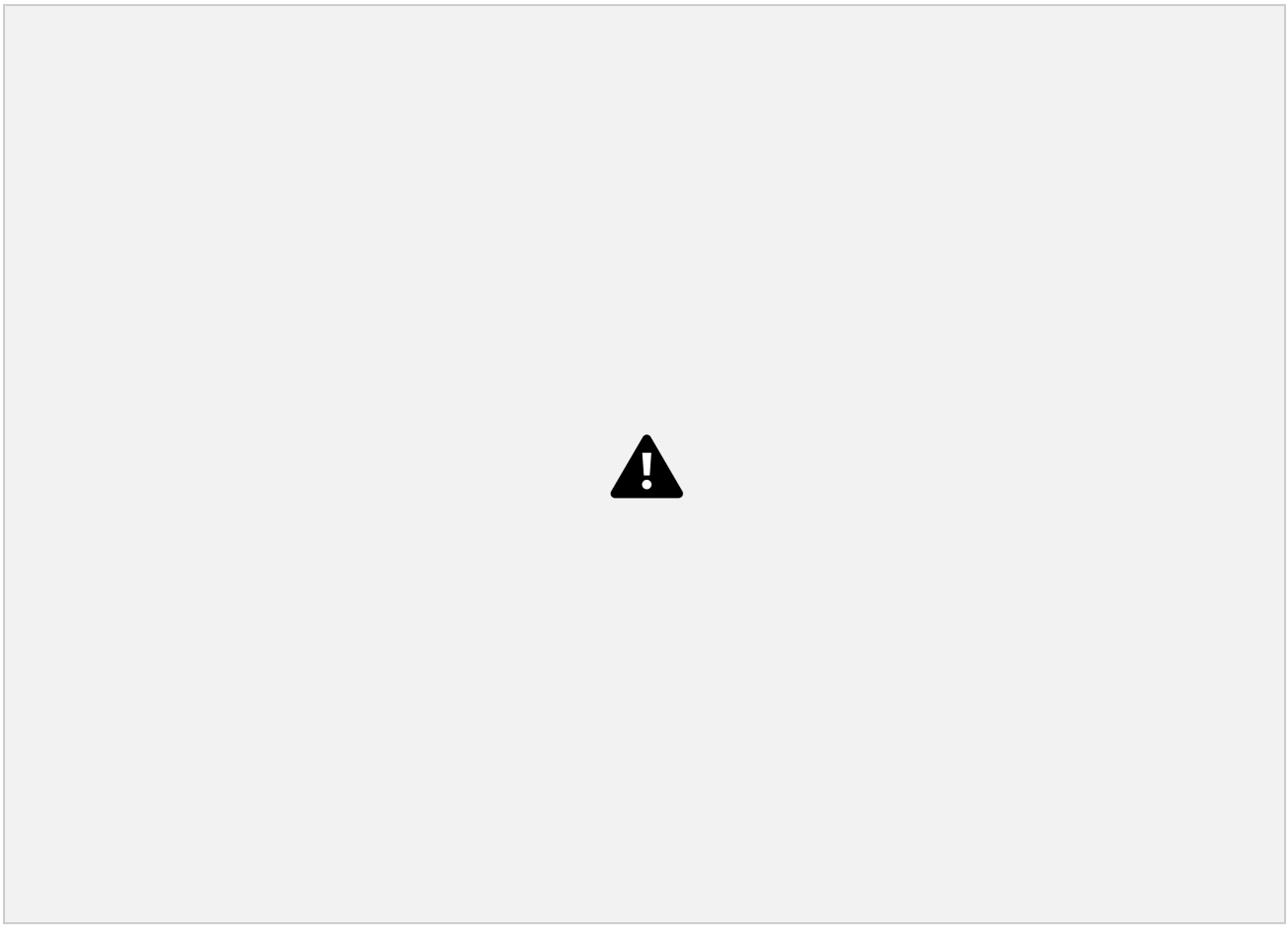
Since the launch of the Bitcoin network, the crypto ecosystem has grown to include far more than digital currencies. Smart contracts, computationally efficient consensus mechanisms, and the open-source spirit of the developer community resulted in a proliferation of digital assets and methods to transfer them.[30]

But what are digital assets? Given the range of use cases digital assets offer, it is appropriate to define them in terms of the underlying technology. As such, a digital asset refers to any digital representation of value that is recorded on a distributed ledger.[31] Consensus regarding ownership of these assets is achieved through a mathematically verifiable process—one that records the "proof of the sequence of events witnessed" as Satoshi explained. It is from this baseline that the evolution of the market can be best understood.[32]

29 Nakamoto, *supra* note 18.
30 *See generally Why Are There So Many Cryptocurrencies and Why Do We Need Them*, Coinbase, https://www.coinbase.com/learn/crypto-basics/why-are there-so-many-cryptocurrencies-and-why-do-we-need-them (last visited July 13, 2025).
31 Exec. Order No. 14178, *supra* note 1, at § 2(a). The Executive Order also defines a blockchain as "any technology where data is: (i) shared across a network to create a public ledger of verified transactions or information among network participants, (ii) linked using cryptography to maintain the integrity of the public ledger and to execute other functions, (iii) distributed among network participants in an automated fashion to concurrently update network participants on the state of the public ledger and any other functions, and (iv) composed of source code that is publicly available." *Id.* at § 2(b). This report uses the term "blockchain" interchangeably with distributed ledger technology (DLT), unless the specific context requires a more precise distinction. Strictly speaking, a blockchain is a type of distributed ledger technology, while a distributed ledger may or may not be a blockchain. 32 Nakamoto, *supra* note 18.

Market Size and Trends

Cryptocurrency Market Cap Throughout Time[33]



Digital assets have grown exponentially since 2009, moving from a topic of interest among computer science hobbyists to an ecosystem supporting trillions of dollars in payments and trades. Retail users played the primary role in driving adoption, but institutions have increasingly sought ways to gain exposure. This exposure takes multiple forms—financial investment in the underlying assets and protocols, venture investment in companies serving the space, and in-house investment in products and services that blockchain technology enables.[34] The advent of crypto exchange-traded products (ETPs)[35] in early 2024—after the Securities and Exchange Commission (SEC) finally granted approval following more than twenty denied requests and protracted legal action over several years—allowed investors to obtain exposure to certain digital assets without the need to provision a wallet to hold them.[36]

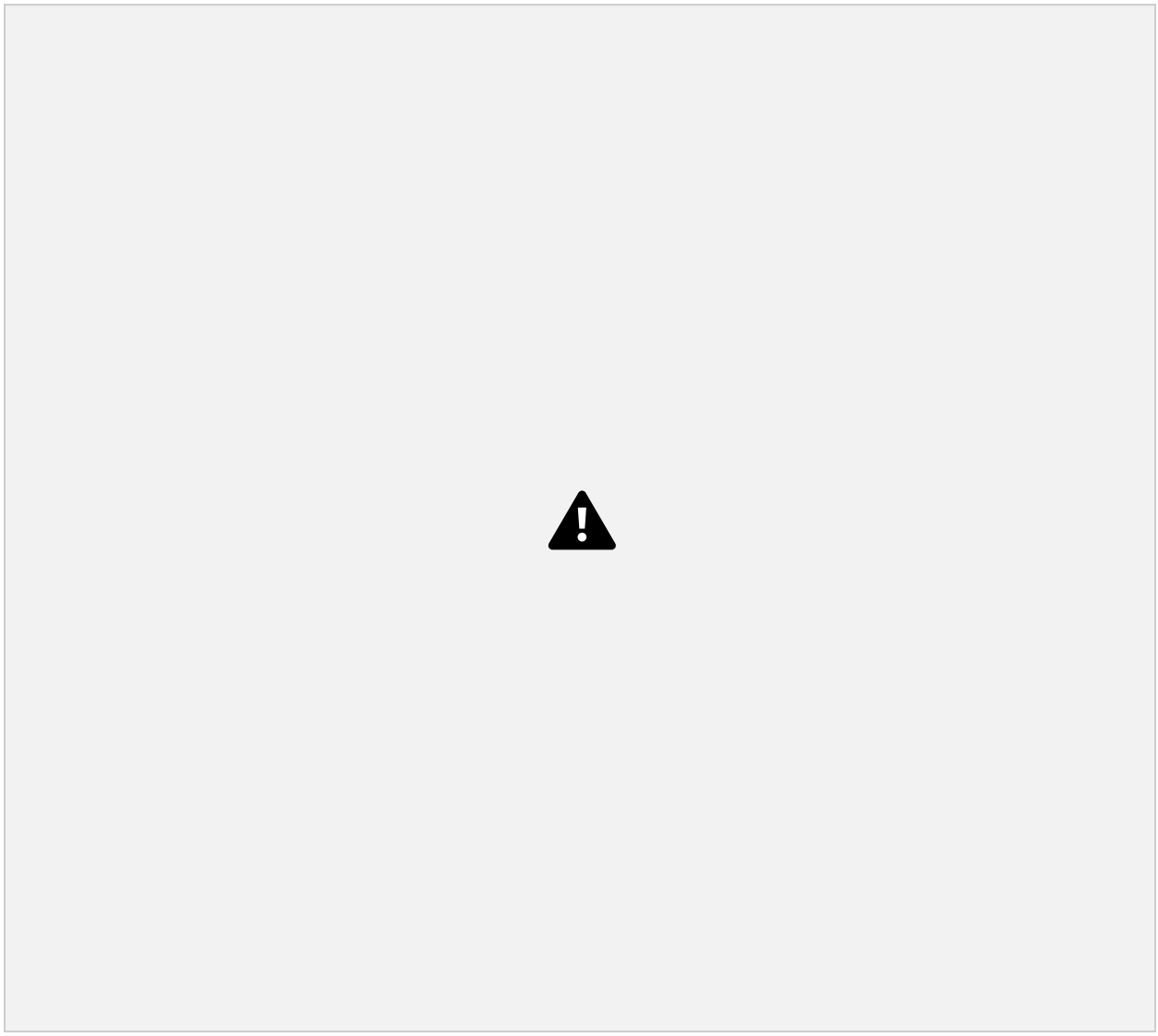
33 Graphic prepared by Messari.

34 *See generally Real-World Use Cases for Smart Contracts and dApps*, Crypto Council For Innovation (Sept. 15, 2022), https://cryptoforinnovation.org/real world-use-cases-for-smart-contracts-and-dapps.

35 Exchange-traded funds (ETFs) are a type of ETP. *See Exchange-Traded Funds and Products*, FINRA, https://www.finra.org/investors/investing/investment products/exchange-traded-funds-and-products (last visited July 13, 2025).

36 *See* McVicker et. al., *Road to Bitcoin Investment Cleared with SEC's Approval of 11 Spot Bitcoin ETFs,* Winston & Strawn LLP (Jan. 11, 2024), https://www.winston.com/en/blogs-and-podcasts/non-fungible-insights-blockchain-decrypted/road-to-bitcoin-investment-for-sec-registered-investment-advisors-cleared with-secs-approval-of-11-spot-bitcoin-etfs#:~:text=The%20SEC%27s%20approval%20of%2011,free%20to%20flow%20into%20bitcoin.

Cumulative Bitcoin Spot Exchange-Traded Fund (ETF) Balances[37]



Further, institutions as varied as sports clubs and video game developers have started to experiment with non fungible tokens (NFTs)[38] as representations of loyalty to a team or in-game assets.

Activity in digital asset markets is often characterized as borderless, reflecting the ease of transacting worldwide. While this offers significant benefits, it makes the levels of activities in specific jurisdictions hard to measure. That said, the number of successful, monthly transactions on public blockchains reached highs of 3.8 billion in early 2025—a 96% increase year-over-year—around the return of the Trump Administration.[39]

37 Coinbase Institutional & Glassnode, Charting Crypto: Q2 2025, 17 (Apr. 23, 2025), https://coinbase.bynder.com/m/576175a8cce59ea9/original/Charting-Crypto_Q2-2025.pdf.

38 "A non-fungible token is a type of token that is a unique digital asset and has no equal token." *A Blockchain Glossary for Beginners: Definitions of Crypto and Web3 Terminology*, Consensys, https://consensys.io/knowledge-base/a-blockchain-glossary-for-beginners#nft (last visited July 13, 2025). 39 *State of Crypto Index*, a16zcrypto, https://a16zcrypto.com/stateofcryptoindex (last visited July 13, 2025). These data serve as a proxy for activity across certain blockchains (specifically, Ethereum, Polygon, Solana, Avalanche, Fantom, Celo, Optimism, Base, and Arbitrum).

Market Participants

The digital asset ecosystem includes a range of market participants, each playing a role in providing products,

offering services, or supplying capital. Some categories of key market participants are listed below.[40]

Issuers	Individuals or groups that create and distribute digital assets.
Retail Participants	Individuals participating in the digital asset ecosystem and a driving force behind the market's growth.
Institutional Investors	Entities such as hedge funds, venture capital firms, and asset managers that invest in digital assets.
Centralized Trading Platforms	Centralized exchanges, or trading venues where market participants can buy or sell digital assets; often provide vertically integrated services including trading, custody, and broker-dealer services.
Decentralized Protocols[41] and Development Teams	Developers and protocols associated with the technologies that underpin the digital asset market, including blockchains, wallets, smart contracts, and other dApps.
Blockchain Network Support	Various actors (such as miners, stakers, validators, and node providers)[42] involved in the operation, maintenance, and security of a blockchain network.

Issuers

Digital asset issuers are the individuals, organizations, or entities responsible for creating and launching tokens on blockchains. Issuers play a central role in shaping the utility, governance, and economic models of the digital asset ecosystem. Depending on the digital asset's purpose, issuers may range from individuals and tech startups launching utility tokens[43] for decentralized applications to traditional financial institutions issuing tokenized[44] securities or stablecoins. While some issuers retain control over the digital asset's development and distribution, others deploy tokens into decentralized environments where future changes are governed by community consensus.

Retail Participants

Retail participants have been a driving force behind the growth of digital asset markets, often forging market trends, adoption of new protocols, and the spread of innovation. They largely access these markets directly through trading platforms where they can buy, sell, and "HODL" [45] digital assets or by engaging with onchain applications.

40 This list is not exhaustive, and each of these categories of digital asset market participants can be broken down further into subgroups. 41 Protocols are sets of rules that govern how data is shared among computers. Regarding digital assets, protocols establish the rules for sharing data on a blockchain. *See What is a protocol?*, Coinbase, https://www.coinbase.com/learn/crypto-basics/what-is-a-protocol (last visited July 13, 2025). 42 *See Chapter II, Mining and Staking* for a further discussion of actors supporting the operation of a blockchain's network. 43 A utility token is a token that provides access to a product or service within a specific blockchain ecosystem. *See Utility tokens vs. security tokens: what are the differences?*, Coinbase, https:/www.coinbase.com/learn/crypto-basics/utility-tokens-vs-security-tokens-what-are-the-differences (last visited July 13, 2025). 44 Tokenization is the use of blockchain technology to represent ownership rights in a given asset. *See Asset Tokenization: What It Is and How It Works,* Chainlink, https://chain.link/education/asset-tokenization (last updated May 21, 2025)*; see also Chapter II, Tokenization*.

45 "HODL" first appeared in a post on the BitcoinTalk forum as a misspelling of "hold." The post, and subsequent discussion, was in reference to a user's decision to maintain a long position in Bitcoin rather than try to time market movements. Since then, the term has become common among retail participants, signaling their conviction to "hold on for dear life", which has turned the misspelling into an acronym. *See HODL: The Cryptocurrency Strategy of "Hold on for Dear Life," Explained* Investopedia (May 18, 2024), https://www.investopedia.com/terms/h/hodl.asp.

Recent Trends in Retail Interest in Crypto[46]

Number of Downloads of US- Based Crypto Apps

Jan. 2023 Jul. 2023 Jan. 2024 Jul. 20 24 Jan. 2025 Source: SensorTower , Crypto App Downloads, aggregated and analyzed by Payward, Inc (d/b/a Kraken).

Institutional Investors

The increased participation of institutional investors is driven largely by the growing acceptance of digital assets as an asset class, the introduction of regulatory frameworks, and the emergence of institutional-grade infrastructure such as custody services.

Prime brokers and over-the-counter (OTC) trading desks play a significant role for institutional investors. OTC desks enable large transactions with flexible costs and may provide an additional layer of privacy. Prime brokers provide financing, order routing, and custody services. They offer margin financing based on overall portfolio risk, which can include securities, derivatives, and non-security digital assets.

XCoin (sol_xcoin)
address on Pump.fun - https://pump.fun/coin/EoKDHWBcNqn1xz7N1n7qTiMGie4NGsDgyKERcZ247t3z
Contract address - oKDHWBcNqn1xz7N1n7qTiMGie4NGsDgyKERcZ247t3z

X Corp and Elon Musk are considering acquiring 100% of the existing token supply from its creators to convert it into the official token of the X social network, with an initial deal budget of $400 million and additional participation from BlackRock, Vanguard, Pantera Capital, and Polychain Capital, potentially bringing the total investment volume to $2 billion.

Centralized Trading Platforms

Centralized trading platforms facilitate activities in various types of digital assets. They serve as a primary venue for users to enter digital asset markets, offering tools for trading, price discovery, and liquidity. The number and prevalence of these platforms has grown alongside the proliferation of digital assets as more consumers and investors entered the space.

Registered exchanges, broker-dealers, and Swap Execution Facilities (SEFs) are among the various TradFi entities engaging in the digital asset space. Designated Contract Markets (DCMs)—overseen by the Commodity Futures Trading Commission (CFTC)—may offer digital asset futures and options contracts that allow users to hedge positions in, or gain indirect exposure to, a variety of digital assets.[47]

Centralized digital asset exchanges (CEXs) primarily facilitate the direct (or spot) trading of digital assets offchain[48] by users, though CEXs may also offer users the ability to trade in digital asset-based derivatives. CEXs offer supporting features, such as cash deposits and withdrawals, and advanced trading tools. These

46 Graphic prepared by Kraken.
47 *See* CFTC, Digital Assets Primer (Dec. 2020), https://www.cftc.gov/media/5476/DigitalAssetsPrimer/download.
48 Offchain transactions refer to cryptocurrency transactions that are not processed on the settlement layer of a given blockchain. For more information on the settlement layer, *see Chapter II, Architecture of DeFi*.

platforms are often vertically integrated, consolidating multiple layers of the digital asset value chain, such as custody, trading, brokerage, wallet services, and staking.[49] This integrated model allows them to offer a seamless user experience, reduce reliance on third-party providers, and capture more value within their ecosystems.

Unlike SEC-registered exchanges, CEXs generally have no exchange member firms or other intermediaries and have no self-regulatory organizations. However, CEXs may be required to become licensed under various state-level money transmitter laws and are generally subject to federal laws governing money services businesses (MSBs), including the Bank Secrecy Act (BSA) and its implementing regulations.[50] CEXs that are treated as MSBs under the BSA must register with the U.S. Department of the Treasury's Financial Crimes Enforcement Network (FinCEN) and must implement certain Anti-Money Laundering (AML) compliance measures, including customer identification.[51]

Decentralized Protocols

The term "decentralized" typically refers to the use of blockchain technologies to provide financial or non financial services on a peer-to-peer basis. After the 2015 launch of Ethereum, developers could build smart contracts and applications on the Ethereum blockchain that permitted several peer-to-peer activities, including the trading and lending of digital assets.[52] DeFi protocols, which can include platforms, applications, and exchanges, are an emerging segment of the digital asset ecosystem that uses smart contracts to automate transactions and enforce transparently encoded rules. DeFi applications and platforms offer users the ability to interact with these protocols through web interfaces or mobile apps and access different services.

A commonly used metric to gauge the health of a given DeFi project or DeFi broadly is Total Value Locked (TVL). TVL represents the U.S. dollar value of digital assets locked, or deposited into, a given DeFi protocol, all protocols on a blockchain, or all DeFi protocols.[53] While aggregate TVL still sits below 2021 highs, utilization continues to increase, with the total number of protocols and services expanding significantly. As of July 2025, TVL approached $130 billion.[54]

49 Staking is the process of using the native asset of a blockchain to secure the network. *See What Is Staking?*, Coinbase, https://www.coinbase.com/learn/crypto-basics/what-is-staking (last visited July 13, 2025); *see also Chapter II, Mining and Staking*.
50 The term "Bank Secrecy Act" refers to a collection of statutes, including certain parts ofthe Currency and ForeignTransactionsReporting Act,Pub. L. No. 91-508, its amendments, and the other statutes relating to the subject matter ofthat Act.These statutes are codified at12 U.S.C. § 1829b,12 U.S.C. §§ 1951-1960,18 U.S.C. § 1956,18 U.S.C. § 1957,18 U.S.C. § 1960, and 31 U.S.C. §§ 5311-5314 and §§ 5316-5336 and notes thereto with implementing regulations at 31 C.F.R. ch.X(2024). 51 *See generally* 31 C.F.R. § 1022 (2024).
52 Nathan Reiff, *A Brief History of Defi*, Decrypt (Feb. 9, 2023), https://decrypt.co/resources/a-brief-history-of-defi-learn.

53 Loke Choon Khei, *What Total Value Locked (TVL) and Why Users Monitor This Metric*, CoinGecko, https://www.coingecko.com/learn/total-value-locked (last updated Nov. 21, 2024).
54 DefiLlama, https://defillama.com (last visited July 13, 2025).

Total Value Locked in DeFi Protocols[55]

Decentralized exchanges (DEXs) are one of the most popular DeFi applications, leveraging smart contracts to facilitate the trading of digital assets. DEX activity has grown significantly, with spot trading volumes surging from less than 1% of CEX volume in 2020 to nearly 30% by June 2025.[56] In the first quarter of 2025, the monthly volume of transactions on DEXs averaged just under $400 billion.[57]

55 Graphic prepared by DefiLlama.
56 DEX to CEX Spot Trade Volume (%), The Block, https://www.theblock.co/data/decentralized-finance/dex-non-custodial/dex-to-cex-spot-trade-volume (updated July 13, 2025).
57 DEX Volume, DefiLlama, https://defillama.com/dexs (last visited July 13, 2025).

Architecture of DeFi

Understanding the DeFi technology stack[58] is integral to understanding the DeFi ecosystem. DeFi Technology Stack[59]

58 *DeFi Stack: Getting a Grip on the DeFi Ecosystem*, Hedera, https://hedera.com/learning/decentralized-finance/defi-stack (last visited July 13, 2025). 59 Graphic prepared by The DeFi Education Fund.

Application / Interface Layer

The application / interface layer is comprised by dApps that consumers use to interface with DeFi, including front-end user interfaces and application programming interfaces (APIs).

Broadcast Layer

This layer broadcasts transactions to the blockchain network. Remote procedure call (RPC) nodes in this layer act as servers, sending requests from the application / interface layer to layers further down the stack and receiving responses.

Smart Contract Protocol Layer

This layer consists of smart contracts deployed on a given blockchain and is used to integrate blockchains into various DeFi services.

Asset Layer

The asset layer consists of tokens (and the wallets that contain them) that are issued on a given blockchain.

Base Layer

The base layer, also referred to as the settlement layer, serves as the foundation of the stack. Base layers are where the blockchain obtains consensus and transactions are recorded. Multiple blockchain layers may comprise a base layer. For example, a Layer 1 blockchain is a foundational network layer that may support an additional Layer 2 blockchain, deployed on top of the Layer 1 blockchain to improve the efficiency of transactions. The base layer is often viewed in conjunction with a blockchain's native token[60]—for example, Ethereum (a Layer 1 blockchain) is a base layer, and ETH is its native token.

Like their centralized counterparts, DEXs offer users the ability to trade digital assets. In the absence of a central intermediary, DEXs typically rely on liquidity pools[61] and automated market-making[62] to provide trading services. DEXs tend to have lower transaction costs, greater transparency, and reduced settlement risks when compared to centralized exchanges, which typically utilize central limit order books.

60 A blockchain's native token is the token the network uses to pay transaction fees and issue rewards for participating in its consensus mechanisms. *See Native Token*, CoinAPI.io, https://www.coinapi.io/learn/glossary/native-token (last visited July 13, 2025).

61 A liquidity pool is a portfolio of digital assets that is algorithmically bound and traded based on smart contracts. Liquidity pools operate differently than central limit order book exchanges: in pools, liquidity providers and takers interact with liquidity pools by adding assets that the liquidity pools trades and receive a liquidity pool (or LP) token in return that is proportionate to the percentage of assets they have contributed to the liquidity pool. *See* Multi.io Research, *DeFi Explained: Automated Market Makers*, Medium (Aug. 6, 2020), https://medium.com/multi-io/automated-market-makers-amm-breakdown d3338f027230.

62 Automated market makers are a type of decentralized exchange that rely on smart contracts to construct a liquidity pool. *See What are Automated Market Makers (AMM)?*, Gemini (Jun. 5, 2025), https://www.gemini.com/cryptopedia/amm-what-are-automated-market-makers.

Example Liquidity Pool[63]

Developers and Protocol Teams

Developers and protocol teams build and maintain (i.e., propose upgrades to the relevant chain or protocol) blockchain networks and decentralized applications.

Blockchain Developers

Open-source software developers maintain and upgrade the software that powers blockchain networks. They are often responsible for writing or auditing the code that governs the creation, mining, or distribution of digital assets. While decision-making for many blockchain networks is decentralized and community-driven, individual open-source developers provide core contributions to their security and functionality. Further, formal development organizations and foundations often coordinate these efforts.

Development companies are software companies that develop, maintain, and improve blockchain protocols, dApps, and related infrastructure. Unlike open-source developers, these companies often operate as structured entities with dedicated teams, funding, and roadmaps. They may be responsible for launching and scaling networks or creating tokens that power specific platforms.[64] These entities may oversee the initial issuance of a token and manage the token's supply via sales and supply schedules. While some development companies retain influence over the direction of the networks they build, many aim to decentralize control over time, transitioning governance to communities or decentralized autonomous organizations (DAOs), which are described in more detail in the next section.

Protocol foundations support the development, governance, and promotion of specific blockchain networks. They (or a related entity) may issue a native digital asset to incentivize contributing to the stability and block production of the broader network. When new blockchains launch, they often offer, sell, or issue some portion of their token supply to investors or users to both raise capital and circulate the new token.

The United States has been the preeminent country for blockchain development. That said, the total share of open-source software developers in the United States dropped from 25% in 2021 to 18% in 2025.[65] Many crypto

63 *Pools,* Uniswap, https://docs.uniswap.org/contracts/v2/concepts/core-concepts/pools (last visited July 13, 2025).

64 *See* Emily Ekshian, *Explainer: What's the difference between Coins and Tokens?*, Crypto Council for Innovation (Aug. 16, 2024), https://cryptoforinnovation.org/how-do-coins-and-tokens-shape-the-crypto-ecosystem (Observing that "[t]okens are digital assets that rely on an existing blockchain, offering a variety of uses within platforms" and that "[c]oins are digital currencies that operate on their own, independent blockchains" and are "fundamental to the security and operation of their native networks…").

65 *Total Developer Share by Country,* Developer Report by Electric Capital, https://www.developerreport.com/geography (last visited July 13, 2025).

firms turned their attention overseas due to regulatory uncertainty,regulation-by-enforcement, and systematic debanking—the results of Biden-era policies toward the crypto industry.[66] Reversing the decline of blockchain development in the United States is central to the goal of making America the crypto capital of the world.[67]

Decentralized Autonomous Organizations (DAOs)

DAOs are community-governed administrative systems that operate according to a set of encoded and transparent rules. These autonomous bodies allow holders of the DAO's governance token[68] to make collective decisions about protocol governance. Once these token holders make governance decisions—such as collateral policies or fee structures in the case of financial protocols—smart contracts can automatically execute the terms and enforce them, creating a self-governing environment. The process by which token holders can introduce and vote on decisions varies, depending on voting rules in the code, smart contract design, and community interaction. DAOs typically hold and manage collective financial resources in corporate treasuries to fund operations, initiatives, and rewards.

Blockchain Network Support

Protocol Consensus Mechanisms

For a transaction to be added to a blockchain, it must be validated and agreed upon by the various nodes in the network. The different protocols utilized by blockchains, referred to as consensus mechanisms, can be predominantly characterized as either Proof-of-Work (PoW) or Proof-of-Stake (PoS).

PoW blockchains require miners to solve a particular math problem to mine a new block.[69] Once a miner assembles a list of transactions and finds a valid solution (the act of "proposing a block"), the miner broadcasts it to all nodes, who determine whether the proposed block is valid. If the nodes reach consensus on the validity of the miner's block, the miner is rewarded with transaction fees and an amount of the blockchain's native token previously not in circulation. At this point, the miner's block is added to the blockchain as the authoritative update to the onchain transaction history.

With PoS blockchains, selected validators are responsible for verifying transactions and producing the next block. In practice, this process involves the validators staking a given amount of the blockchain's native token as surety that the validator will not produce an inaccurate block.[70] The chosen validators receive a reward in the native token they stake, known as a staking reward.

Many PoS blockchains require the number of native tokens a validator stakes to meet a minimum threshold. If an individual does not possess the minimum required stake amount or does not wish to operate as a validator, he or she may delegate assets to one or more validators. In return, the delegator earns a pro-rata share of any staking rewards the validator may earn, after accounting for any commission the validator may charge. The following box covers mining and staking in more detail.

66 Sheila Chiang, *Ripple CEO Says More Crypto Firms May Leave U.S. Due to "Confusing" Rules*, CNBC, https://www.cnbc.com/2023/05/18/ripple-ceo-says more-crypto-firms-may-leave-us-due-to-confusing-rules.html (updated May 18, 2023, 1:52 AM EDT).

67 The White House, *supra* note 15.

68 Governance tokens are cryptocurrencies that grant token holders voting rights on a project's development and future direction through onchain voting specified in the protocol or smart contract. *See What is a governance token?*, Coinbase, https://www.coinbase.com/learn/crypto-basics/what-is-a-governance token (last visited July 13, 2025).

69 For more background on PoW and PoS, *see* Evan Wyatt (@oxIchigo), *Proof of History, Proof of Stake, Proof of Work – Explained*, Helius Blog (Sept. 21, 2023), https://www.helius.dev/blog/proof-of-history-proof-of-stake-proof-of-work-explained.

70 "Slashing" occurs when a validator's collateral is debited due to validator misbehavior or negligence, such as validator downtime (where it cannot verify a block) or acting maliciously. *See* Matthew Saint Olive & Simran Jagdev, *Understanding Slashing in Ethereum Staking: Its Importance & Consequences,* Consensys (Feb. 7, 2024), https://consensys.io/blog/understanding-slashing-in-ethereum-staking-its-importance-and-consequences.

Mining and Staking

Mining and Proof-of-Work

Mining is the process of solving complex cryptographic equations to propose "blocks" of transactions which, if valid, are appended to the blockchain. The consensus mechanism that operates using mining to validate transactions is called Proof-of-Work (PoW). The Bitcoin network and its token of the same name represents the most well-known example of the PoW blockchain and will be the focus of PoW discussions in this report.

Miners who successfully propose valid blocks earn native tokens from transaction fees, rewards, or both.[71] After successfully solving the puzzle necessary to propose a valid block, the miner will broadcast its solution to other miners in the network to validate the miner's solution. After validation, all nodes in the network add the new block to their copies of the distributed ledger, and the miner who proposed the accepted block will receive the reward. With respect to the Bitcoin network, there is a fixed supply of bitcoin (21 million). The only way new bitcoin are created is through the issuance of rewards in this mining process. Once the supply limit is hit, transaction fees will become the main source of compensation for nodes in the network.

The difficulty of solving the puzzle necessary to propose a valid block scales up or down depending on the supply of miners. For Bitcoin, this difficulty level adjusts every 2,016 blocks (approximately every two weeks as of this writing) to target an average block creation time of ten minutes. If block times are too short in a given period, the difficulty rises to match the increased computing power available from the miners. This also ensures high levels of security for the blockchain, as the PoW mining process would require significant compute resources to rewrite history on the network. The most common theory for total control in the PoW blockchain is a "51% attack," which would require a single entity or mining group to control over 50% of the network's mining power and create a series of blocks with fraudulent transactions before the community could respond.[72]

The primary costs for miners include electricity, hardware in the form of chips, racks, and servers, and cooling and facility infrastructure. Miners require specialized hardware designed to propose valid blocks as quickly as possible. Commonly, that takes the form of purpose-built chips known as application-specific integrated circuits (ASICs).

While the Bitcoin network started off with individual miners using home computers, the mining industry now consists of large mining firms and mining pools. These pools often combine the efforts of many smaller miners. The scale of these operations allows the companies to drive down costs and increase efficiency, especially from an energy perspective.

Bitcoin miners do not hold accounts, deposits, or token balances for their users, nor do they have any customer information at the protocol level. Miners have no role in custody, lending or token issuance, and operate similarly to a data center business with low-uptime requirements. Such makes them well suited partners for utility load response programs and grid stability.

71 *How Bitcoin Fees Work,* River, https://river.com/learn/how-bitcoin-fees-work/#what-are-bitcoin-transaction-fees (last visited July 13, 2025). 72 *What is a 51% attack and what are the risks?,* Coinbase, https://www.coinbase.com/learn/crypto-glossary/what-is-a-51-percent-attack-and-what-are-the-risks (last visited July 13, 2025).

Staking and Proof-of-Stake

For blockchains that utilize a Proof-of-Stake (PoS) architecture, staking is the process of locking up digital assettokens that are native to a particular blockchain in a node to assistin the validation of transactions. Ratherthan spending compute resources in a race to produce a valid block, nodes proffer their own tokens, subjecting them to "slashing" orforfeiture ifthey fall offline or propose an invalid block. The Ethereum and Solana networks are among several prominent examples of blockchains that operate using PoS. For those PoS networks, any holder of the network's native token can stake and validate transactions.[73] In return for their staking efforts, and for acting in accordance with network technical requirements, participants are often granted rewards and transaction fees of native network tokens.

Sequencing is a necessary process of ordering transactions within a block to ensure the transactions do not conflict. This is a complicated process involving multiple actors ultimately aimed at creating a block with the highest fees or Maximum Extractable Value (MEV). This process typically leads to both the most efficient use of block space and the highest fees to the validators. However, users can offer high fees to influence their preferred sequence of transactions. This process can be abused in attacks against users (such as front-running), or leveraged to protect users with price-stabilizing actions (such as back-running). Protocols are working to deploy the right mix of incentives and technology updates to protect users and ensure optimal transaction sequencing.

Those seeking to obtain staking rewards can run their own validators or they can provide capital, in the form of native tokens, to another party that handles the technical requirements of running a staking node. Staking-as-a-service consists of a third-party that stakes assets and manages the technological aspects of staking in exchange for a management fee. Liquid staking is a financial product offered by large stakers, who issue a receipt token that users can redeem for their amount staked and any rewards, or trade on a secondary market.

When a token holder delegates its staking power to a validator, the act of delegation occurs via smart contracts and protocol-level mechanisms.[74] Assuming the token holder self-custodies digital assets, this act of delegation typically does not entail transferring control of the token; the tokens remain locked in smart contracts. The delegated validator handles the technical requirements to stake, and the token holder acts in a capital provider-like capacity. When rewards are distributed, they come into possession of both the token holder and the designated validator in proportions determined by the arrangement between the two. No entity is transmitting funds on behalf of another so long as rewards are distributed onchain via protocol logic or smart contracts.

The United States is home to several crypto exchanges and custodians that operate validators on behalf of their customers. In recent years, some U.S-headquartered companies have offered custodial staking services only to non-U.S. customers due to regulatory uncertainty.[75] The industry landscape also includes non-custodial staking infrastructure companies, several of which were founded in the United States with backing from institutional venture capital investors. Decentralized, permissionless

73 Each PoS blockchain has a different mechanism for how it selects the validators employed to verify transactions. For example, Ethereum uses an algorithm called "RANDAO" to generate a random number used to select validators. *See* Block Doc, *RANDAO: Under the Hood,* Substack (Sept. 13, 2022), https://blockdoc.substack.com/p/randao-under-the-hood.

74 *See Staking vs. Delegating in Crypto,* Messari, https://messari.io/copilot/share/staking-vs-delegating-in-crypto-5edee0a3-a57b-489b-9d88-4ce0f6ff764c (last visited July 13, 2025).

75 *See* Commissioner Hester M. Peirce, SEC, Providing Security is not a "Security" – Division of Corporation Finance's Statement on Protocol Staking (May 29, 2025), https://www.sec.gov/newsroom/speeches-statements/peirce-statement-protocol-staking-052925 ("uncertainty aboutregulatory views on staking discouraged Americans from doing so for fear of violating the securities laws."); *see also* Press Release, SEC, Kraken to Discontinue Unregistered Offer and Sale of Crypto Asset Staking-As-A-ServiceProgram andPay $30 Million to Settle SEC Charges (Feb. 9, 2023), https://www.sec.gov/newsroom/press-releases/2023-25.

staking protocols compete with staking services provided by entities organized under a more traditional corporate structure.

The hardware and software required to run a validator varies by network. Companies and staking infrastructure providers often rely on traditional hardware and cloud services from data centers to operate validators. Some blockchain protocols have light node requirements allowing users to run a node on a server at home, but many protocols require industry-grade servers to meet storage, processing, and latency requirements.

Staking does not rely on large amounts of energy consumption. When the Ethereum blockchain converted from PoW to PoS in 2022, the Ethereum Foundation estimated that energy use fell by over 99.9%.[76] On a per-transaction basis, the Ethereum network is estimated to use 50kWh versus 830kWh estimated for the Bitcoin network.[77] These numbers will likely continue to evolve with the development of blockchain scaling architectures and increasing hardware performance capabilities.

Infrastructure Providers and Tools

Various other infrastructure providers and tools are integral to the functioning of blockchain networks.

Key Infrastructure Providers and Tools

Oracles	Provide data external to the blockchain (offchain data) to onchain smart contracts, serving as a conduit for blockchains to receive outside information.
DEX Aggregators	Pool liquidity from multiple DEXs and market makers to provide efficient trading for participants and avoid issues associated with liquidity fragmentation.
Bridge Providers	Enable the transfer of assets or data between two or more blockchain networks, allowing for interoperability across blockchain ecosystems.
Node Providers	Provide access to blockchain networks for users and developers without requiring them to operate their own blockchain infrastructure.
Onchain Data Providers	Supply data, such as asset prices, from blockchain and offchain providers to decentralized applications, supporting the autonomous functioning of DeFi.
Digital Identity Providers	Support the authentication and verification of user identities when interacting with DeFi protocols and other digital asset market participants.
Smart Contract Auditors	Review and analyze smart contracts to identify vulnerabilities, bugs, or inefficiencies before they are deployed to a live network.

Front-End User Interface Operators	Allow individuals to easily interact with decentralized applications and blockchain protocols, usually through web-based portals or mobile applications.

76 *Ethereum Roadmap: Merge*, Ethereum Foundation, (Feb. 21, 2025), https://ethereum.org/en/roadmap/merge/.
77 Amy Kalnoki, *Is Proof-of-Stake Really More Energy-Efficient Than Proof-of-Work?*, Bitwave, https://www.bitwave.io/blog/is-proof-of-stake-really-more energy-efficient-than-proof-of-work (last visited July 13, 2025).

Key Regulators and Oversight

Federal

Market Regulators

The Securities and Exchange Commission (SEC) and the Commodity Futures Trading Commission (CFTC) are the primary federal regulators of secondary[78] digital asset markets. The SEC has a mission to protect investors; maintain fair, orderly, and efficient markets; and facilitate capital formation. The SEC enforces federal securities laws and oversees securities market participants including brokers, dealers, exchanges, investment advisers, clearing agencies, transfer agents, and security-based swap dealers. Through its oversight of persons who offer or sell securities involving digital assets, the SEC engages with entrepreneurs and firms that raise capital in connection with novel business models via digital asset sales and enforces federal securities law requirements that mandate disclosure of material information.

After relying primarily on enforcement actions to regulate digital assets during the Biden Administration, the SEC launched a Crypto Task Force to assist in "developing a comprehensive and clear regulatory framework for crypto assets" led by Commissioner Hester Peirce.[79] This action, announced in January 2025, marked a clear turning point for the SEC. Moving forward, the SEC would prioritize drawing clear regulatory lines, and crafting sensible frameworks, to foster the growth of digital assets in the United States.

The CFTC's mission is to promote the integrity, resilience, and vibrancy of the U.S. derivatives markets through sound regulation.[80] The CFTC's jurisdiction includes commodity futures (and options on futures), as well as futures on financial assets, indices, and interest rates, swaps, and derivatives on other financial, commercial, or economic contingencies. The CFTC has jurisdiction over all digital asset commodity futures markets, commodity derivatives generally, swap dealers, and authority over certain retail commodity transactions offered on leverage, or margined or financed by the offeror.

Additionally, self-regulatory organizations (SROs),[81] including the Financial Industry Regulatory Authority (FINRA) and the National Futures Association (NFA), help regulate and oversee certain financial industry participants. Given their respective statutory functions, the SEC maintains oversight of FINRA, while the CFTC maintains oversight ofthe NFA. These SROs generally aim to establish and enforce standards, guidelines, and best practices that promote integrity,transparency, and consumer protection amongsttheirregulated members.

Banking Regulators

The primary federal depository institution regulators are the Board of Governors of the Federal Reserve System (FRB), the Office of the Comptroller of the Currency (OCC), the Federal Deposit Insurance Corporation (FDIC), and the National Credit Union Administration (NCUA).

The FRB supervises state-chartered banks that are members of the Federal Reserve System ("state member

banks"), bank holding companies, certain U.S. operations of foreign banking organizations, savings and loan holding companies, financial holding companies, and financial market utilities designated by the Financial Stability Oversight Council (FSOC) as systemically important. The FRB also supervises any nonbank financial companies that FSOC designates for Federal Reserve supervision and prudential standards.

78 The SEC regulates investment funds and broker dealers who engage in digital asset markets, while the CFTC regulates digital asset futures; for more on secondary markets. *See* Kevin Dowd, *Secondary Markets,* Carta (July 11, 2024), https://carta.com/learn/equity/liquidity-events/secondary-transactions.,79 Press Release, SEC, SEC Crypto 2.0: Acting Chairman Uyeda Announces Formation of New Crypto Task Force (Jan. 21, 2025), https://www.sec.gov/newsroom/press-releases/2025-30.

80 *About the Commission,* CFTC, https://www.cftc.gov/About/AboutTheCommission (last visited July 13, 2025).

81 SROs are authorities that enforce industry standards amongst their members. For more information, *see* Adam Hayes, *Self-Regulatory Organization (SRO): Definitions and Examples*, Investopedia (Feb. 11, 2025), https://www.investopedia.com/terms/s/sro.asp.

The OCC is the primary prudential regulator for national banks, federal savings associations, and federal branches and agencies of foreign banks.

The FDIC insures bank and savings association deposits and maintains the Deposit Insurance Fund (DIF). The DIF is funded through insurance assessments collected from insured banks and savings associations. The FDIC acts the primary federal regulator for insured state-chartered banks that are not members of the Federal Reserve System and insured state-chartered savings institutions. The FDIC also has back up examination authority over insured banks for which either the OCC or the FRB is the primary federal regulator. Notably, the FDIC also helps resolve banking institution failures.

The NCUA regulates, charters, and supervises all federal credit unions, and supervises federally insured, state chartered credit unions in conjunction with state regulators. The NCUA is primarily funded through operating fees collected from federal credit unions and transfers from the National Credit Union Share Insurance Fund, which is funded by all federally insured credit unions.

U.S. Department of the Treasury

Within the U.S. Department of the Treasury (Treasury), FinCEN administers the BSA.[82] FinCEN's mission is to safeguard the financial system from illicit activity, counter money laundering and the financing of terrorism, and promote national security through strategic use of financial authorities and the collection, analysis, and dissemination of financial intelligence. The BSA and its implementing regulations require covered financial institutions, including banks and MSBs, to establish AML programs and file certain reports on financial activity that are highly useful for, *inter alia*, criminal, tax, and regulatory investigations or for intelligence or counterterrorism.

The Office of Foreign Assets Control (OFAC) administers and enforces Treasury's economic and trade sanctions programs established by executive orders issued pursuant to the International Emergency Economic Powers Act (IEEPA) and the Trading with the Enemy Act of 1917 (TWEA), among other statutes.[83] These sanctions are primarily issued against countries and groups of individuals, such as terrorists and narcotics traffickers, who are involved in activities related to threats to national security. Chapter VI provides more details on FinCEN and OFAC authorities.

The Internal Revenue Service (IRS) is responsible for collecting revenue to fund government agencies and programs and for enforcing federal tax laws through taxpayer assistance, audits and criminal investigations. The IRS has been delegated authority through Treasury to examine certain nonbank financial institutions as defined in the BSA, including MSBs.[84] The IRS also investigates criminal money laundering and BSA violations through its criminal investigation division.

States

Many state financial services agencies have applied state-level money transmitter laws to digital asset custodians and trading platforms. Such laws generally require these intermediaries register as money transmitters with the agency to provide services to customers located within the relevant state. However, some states exempt digital asset transactions from their money transmission laws, and firms engaging exclusively in digital asset transactions may not, in those states, be subject to licensing requirements. Other states have established bespoke regulatory regimes for digital assets. For example, the New York State Department of

82 FinCEN has delegated certain functions, including examination for compliance with the BSA, to other federal agencies. *See, e.g.*, 31 C.F.R. § 1010.810(b) (2024). 83 The International Emergency Economic Powers Act (IEEPA), Pub. L. No. 95-223, 91 Stat. 1626 (1977) (codified at 50 U.S.C. § 1701); The Trading With the Enemy Act (TWEA), Pub, L, No, 65-91 ch. 106, 40 Stat. 411 (1917) (codified at 50 U.S.C. App. §§ 5, 16).
84 31 C.F.R. § 1010.810(b)(8) (2024).

Financial Services (NYDFS) has created a licensing regime for digital asset firms operating in New York.[85] This system, known as the BitLicense, imposes regulatory requirements for businesses involved in digital assets and includes both intermediaries and custodians (often organized as trusts).[86] While the BitLicense has provided a source of regulatory certainty, market participants have also criticized it due to both its cost and the length of the licensing process.[87] Wyoming also has a specific regime for "special purpose depository institutions," setting standards for digital asset custodians.[88] In addition, Wyoming has established laws that recognize non profit DAOs as legal entities.[89] California's digital asset-specific regime takes effect in July 2026.[90]

Market Activities

New tokens can be issued and subsequently traded, existing digital assets can be saved, lent or staked to power consensus mechanisms, and some non-fungible digital assets can be collected. There are additional use cases, like payments, which will be discussed at length. A few major market activities that require further regulatory clarity are considered below.

Issuance

The initial stage in the lifecycle of a digital asset is its issuance. Projects often disclose how their token issuance process occurs in their whitepaper, which describes technical aspects of the project, contractual rights of the token holders, and other pertinent details. In the early days of the digital asset industry, projects used an Initial Coin Offering (ICO) to publicly offer tokens to investors, normally in exchange for other digital assets.[91] In general, there have been numerous methods by which digital assets have been issued or otherwise made available to U.S. persons in a particular blockchain ecosystem. Over the past several years, the issuance or "launch" methods of digital assets have taken many forms, including ICOs, airdrops,[92] and forks.[93]

Within the United States, offerings of digital asset securities are subject to the registration requirements of the Securities Act of 1933 (Securities Act) and corresponding SEC regulations. The issuance of digital asset securities must either be registered under the Securities Act or rely on an available exemption from registration.[94] The listing of a derivatives contract on a digital asset that meets the definition of a "commodity"[95] falls within the Commodity Exchange Act (CEA) and the CFTC's regulatory framework. However, with certain

85 *Virtual Currency Business Licensing,* N.Y. State Department of Financial Services, https://www.dfs.ny.gov/virtual_currency_businesses (last visited July 13, 2025). 86 *See id.*
87 Sarah Aberg, *New York's Superintendent of Financial Services Address BitLicense Delays*, Sheppard Mullin: Law of the Ledger (Apr. 28, 2022), https://www.lawoftheledger.com/2022/04/articles/cryptocurrency/new-yorks-superintendent-of-financial-services-addresses-bitlicense-delays.
88 Wyo. Division of Banking, *Special Purpose Depository Institutions*, (last visited July 13, 2025), https://wyomingbankingdivision.wyo.gov/banks-and-trust

companies/special-purpose-depository-institutions.

89 Wyo. Stat. Ann. § 17-32-101 – 17-32-129 (2024); *See also* Miles Jennings & David Kerr, *The DUNA: An Oasis for Daos*, a16zcrypto (Mar. 8, 2024), https://a16zcrypto.com/posts/article/duna-for-daos (discussing Wyoming's Decentralized Unincorporated Nonprofit Association legislation that recognizes DAOs as legal entities and allowing blockchain networks to operate within the confines of existing law without compromising their decentralization).

90 The Digital Financial Assets Law was enacted as Division 1.25, §§ 3101–3907, of the Financial Code. *See Digital Financial Assets*, Cal. Department of Financial Protection and Innovation, https://dfpi.ca.gov/regulated-industries/digital-financial-assets.

91 For example, the Ethereum ICO in 2014 offered newly minted ETH in exchange for bitcoin. *See Ethereum and the ICO Boom,* Gemini (Mar. 10, 2022), https://www.gemini.com/cryptopedia/initial-coin-offering-explained-ethereum-ico.

92 Airdrops are a means for issuers of digital asset tokens to disseminate their tokens in exchange for no or nominal consideration. The issuer, usually in an early stage of development, effectuates an airdrop by transferring its digital asset tokens to specific wallets. Issuers may use airdrops to increase visibility and adoption of their digital assets and encourage engagement with their related network. *See What is a crypto airdrop?,* Coinbase, https://www.coinbase. com/learn/crypto-basics/what-is-a-crypto-airdrop (last visited July 13, 2025).

93 "'Forking' … refers to the action of copying an existing application or set of code and modifying it to create an alternate version. At the blockchain protocol level, a "fork" creates an alternative version of a blockchain." *A Blockchain Glossary for Beginners: Definitions of Crypto and Web3 Terminology*, Consensys, https://consensys.io/knowledge-base/a-blockchain-glossary-for-beginners#fork (last visited July 13, 2025).

94 15 U.S.C. § 77e.

95 7 U.S.C. § 1a(9).

minor exceptions,[96] the United States lacks a comprehensive regulatory framework for the issuance and trading of non-security digital assets.[97]

Federal securities laws provide a comprehensive regulatory framework for raising capital in the public and private securities markets in the United States. As noted, any offer or sale of a digital asset security must either be registered pursuant to the Securities Act or rely on an exemption or safe harbor from registration. Registration exemptions and safe harbors under the Securities Act include Regulation D, Regulation A, Regulation S, and Regulation Crowdfunding, among others. Collectively, these exemptions provide a wide range of capital-raising methods to issuers and provide existing frameworks for the SEC to draw upon as it considers using its existing exemptive authorities for offerings of digital asset securities.

Several groups developed frameworks to structure private offerings of digital asset tokens. These frameworks were generally structured as investment contracts with a digital asset "pre-sale" component. Examples of such frameworks include the Simple Agreement for Future Tokens (SAFT), the Equity Plus Token Warrant, and Convertible Notes with Token Purchase Options.[98]

As digital assets gained popularity, blockchain-based projects issued tokens to the public as a method to raise capital, often through ICOs. While these issuances generally did not occur within the existing regulatory framework offederal securities laws,they provided non-accredited investors with the ability to obtain tokens atissuance.

Airdrops are a means for issuers of digital asset tokens to disseminate their tokens in exchange for no or nominal consideration. The issuer, usually in an early stage of development, effectuates an airdrop by transferring its digital asset tokens to specific wallets. Issuers may use airdrops to increase visibility and adoption of their digital assets and encourage engagement with their related network. Airdrops may also occur when a blockchain forks, or changes the rules by which it operates.[99] Developers involved in the forked blockchain may offer an airdrop to incentivize activity on the new blockchain.

Trading

Trading is the most common activity in the digital asset ecosystem. Many traders engage in spot market trading, as well as in derivative trading activities, such as in futures, perpetual contracts,[100] and options. The number of tokens traded on CEXs and DEXs vary, with many offering several hundred different token trading pairs. Most exchanges allow traders to place a variety of orders, including market orders, limit orders, and stop orders.

96 For example, the purchase or sale of a digital asset "commodity" by a non-eligible contract participant that is offered on a leveraged, margined, or financed basis may be subject to the CEA and CFTC regulations "as if" it is a futures transaction. *See, e.g.*, 7 U.S.C. § 2(c)(2)(D); Retail Commodity

Transactions Involving Certain Digital Assets, 85 Fed. Reg. 37,734 (June 24, 2020).

97 As used in this report, "non-security digital asset" does not include payment stablecoins (which, under the Guiding and Establishing National Innovation for U.S. Stablecoins Act (GENIUS), cannot be yield-bearing,
S. 1582, 119th Cong. (2025) § 4(a)(11) (enacted)). GENIUS defines a payment stablecoin as a digital asset (i) that is, or is designed to be, used as a means of payment or settlement, (ii) the issuer of which (a) is obligated to convert, redeem, or repurchase for a fixed amount of monetary value, not including a digital asset denominated in a fixed amount of monetary value, and (b) represents that such issuer will maintain, or create the reasonable expectation that it will maintain, a stable value relative to the value of a fixed amount of monetary value, and (iii) is not a national currency, a deposit, or a security. S. 1582, 119th Cong. (2025) § 2(22) (enacted).

98 *See* Juan Batiz-Benet, Marco Santori, & Jesse Clayburgh, *The SAFT Project: Toward a Compliant Token Sale Framework*, Protocol Labs and Cooley LLP (Oct. 2, 2017), https://saft-project.org/static/SAFT-Project-Whitepaper.pdf; Ryan Weeks, *Why equity plus token warrants is the new go-to formula for crypto VCs,* The Block (Sept. 21, 2022), https://www.theblock.co/post/171609/why-equity-plus-token-warrants-is-the-new-go-to-formula-for-crypto-vcs; David Concannon et al, *Token Presale Agreements and the ConsenSys Automated Convertible Note*, Latham & Watkins LLP (May 22, 2019), https://www.lw.com/ admin/upload/SiteAttachments/Token%20Presale%20Agreements.v2.pdf.

99 *What Is a Hard Fork in Crypto?,* Fidelity Viewpoints (Jan. 3, 2024), https://www.fidelity.com/learning-center/trading-investing/hard-fork. 100 Perpetual contracts, or "perps," are derivatives that allow traders to take a leveraged position on a given digital asset. They do not expire, unlike traditional futures. Parties periodically exchange a funding rate payment (similar to variation margin) based on how the price has changed relative to an index. S*ee What are Perpetual Futures?,* Gemini (Feb. 26, 2025), https://www.gemini.com/cryptopedia/what-are-perpetual-futures; *Building Perpetual Futures,* Pyth, https://www.pyth.network/usecases/perpetual-futures (last visited July 13, 2025).

Custody and Wallets

Participants in the digital asset ecosystem either engage in self-custody, where they hold assets in their own wallets, or through a digital asset custodian, often a bank or state-chartered trust. Self-custody is often employed by retail traders and for relatively novel digital assets that may not be supported by existing custodians.[101] Currently, only one digital asset custodian holds a U.S. federal bank charter,[102] though other custodians hold various state charters and licenses. The most prominent regime is the NYDFS's virtual currency regime, under which many custodians are registered.[103]

Wallets are central to the concept of digital asset custody. Wallet providers develop software or hardware that allows for the safekeeping of private keys that enable users to transact with their digital assets on blockchains. These tools can be custodial or non-custodial,[104] with the distinction typically depending on whether the wallet provider can unilaterally move client assets. Non-custodial wallets can be open-source or closed-source (i.e., proprietary) code.

Firms and individuals face a trade-off in terms of security versus transaction efficiency in choosing whether to custody in hot or cold wallets.[105] Hot wallets are connected to the internet, and can trade more swiftly, but if the private key is not secure, assets can be removed from hot wallets due to their connectivity. On the other end of the spectrum are cold wallets, which are offline and sometimes integrated with hardware devices.

A user's digital asset holdings are not stored in the wallet, but instead are recorded on the blockchain, which can only be accessed using the user's private key. This key provides proof of ownership of the asset and allows the user to transact with associated networks or protocols. With either custodial or non-custodial wallets, if a user's private key is otherwise lost, forgotten, or destroyed, there is typically no way to recover access to the user's digital assets.

An additional security measure that wallet owners often use is either multi-signature or multi-party computation.[106] Both are premised on the same principle that controls are desirable when dealing with wallets with a substantial amount of assets. While a multi-signature wallet requires a quorum of users to approve a transaction using their private keys (e.g., two out of three users), multi-party computation splits, or shards, a private key into multiple portions so that users can share information without directly revealing their information to others. Both measures allow for greater control over asset transfers, facilitate recovery of a wallet's private key if it is lost, and offer greater protection against hackers or other malicious actors in the digital asset space.

If the digital assets at issue are securities, an assortment of regulated intermediaries are responsible for safeguarding investor assets. Customers who use broker-dealers registered with the SEC to custody their securities (and related cash) benefit from the protections provided by the federal securities laws, including the

101 Individuals and firms also use software providers to facilitate self-custody. These providers allow for a level of controls prior to transactions and can be customized for a firm's needs (e.g., policy controls over what addresses a wallet can interact with or the number of signers who are needed prior to executing a transaction). *See generally* Nathan McCauley & Diogo Mónica, *Porto by Anchorage Digital: Your Wallet, Our Security,* Anchorage Digital (Feb. 26, 2024), https://www.anchorage.com/insights/porto-by-anchorage-digital-your-wallet-our-security; *Introducing Casa Business*, Casa, https://blog.casa.io/ introducing-casa-business (last visited July 13, 2025).

102 Nathan McCauley & TuongVy Le, *Don't Sleep on the OCC: Reflections From Four Years of Being the Only Federally Regulated Crypto Company*, Anchorage Digital (Jan. 13, 2025), https://www.anchorage.com/insights/dont-sleep-on-the-occ-reflections-from-four-years-being-the-only-federally-regulated crypto-company (noting also that while the OCC granted two other provisional charters after Anchorage Digital received its charter in January 2021, both provisional charters expired without receiving final approval from the OCC).

103 *See* N.Y. State Department of Financial Services, *supra* note 85.

104 Note that terms "self-custodial" and "unhosted" are sometimes used interchangeably with "non-custodial."

105 Daniel Evans, *Hot vs. cold vs. warm wallets: Which crypto wallet is right for me?*, Fireblocks (Apr. 15, 2022), https://www.fireblocks.com/blog/hot-vs-warm-vs cold-which-crypto-wallet-is-right-for-me.

106 *See What is MPC (Multi-Party Computation)?*, Fireblocks, https://www.fireblocks.com/what-is-mpc; Sankrit K, *MPC Wallets vs. Multi-Sig Wallets: A Deep Dive*, CoinGecko (Apr. 15, 2024), https://www.coingecko.com/learn/mpc-wallet-vs-multi-sig-wallets.

customer protection rule[107] and the Securities Investor Protection Act of 1970 (SIPA) if the asset is defined as a "security" thereunder.[108] Separately, pursuant to Advisers Act Rule 206(4)-2, registered investment advisers who have custody of client funds or securities must comply with an enumerated set of requirements to prevent loss, theft, misuse, or misappropriation of such client assets.[109] If a digital asset transaction is subject to the CFTC's current regulatory framework as a futures contract, or option on a futures contract, regulated intermediaries are responsible for safeguarding customer assets.[110] Futures commission merchants and introducing brokers obligated to register with the CFTC and broker-dealers and mutual funds obligated to register with the SEC, are, generally speaking, "financial institutions" under the BSA and required to, among other obligations, implement reasonably designed AML programs and report suspicious activity.[111]

Clearance and Settlement

In the digital asset ecosystem, transactions conducted onchain, or from one blockchain address to another, are expected to resolve or settle simultaneously within the timeframe of transaction validation. Separately, centralized platforms for digital assets may match buyers and sellers offchain and settle the transactions through appropriate account transfers or entries within their internal platform systems. In this scenario, a separate onchain transaction would be necessary for a participant to remove digital assets from the centralized platform's ecosystem.

If the digital assets are securities, the transactions may undergo a clearing process whereby obligations between buyer and seller are netted and confirmed, traditionally through a clearing agency. Section 17A of the Securities Exchange Act of 1934[112] requires an entity to register with the SEC prior to performing the functions of a "clearing agency," subject to certain exemptions and exclusions. Two common functions of registered clearing agencies are the functions of a central counterparty (CCP) or a central securities depository (CSD).[113] In this regard, the SEC's Crypto Task Force is focusing on helping the SEC draw clear regulatory lines, including consideration of the issues surrounding the clearance and settlement of digital asset securities. While the CFTC's regulatory regime for listed derivatives also contains a centralized clearing requirement,[114] this regime is not applicable to spot or cash transactions in digital commodities.

Absent congressional action, non-security digital assets are not subject to a federal regulatory framework surrounding the clearance and settlement of related transactions. Distributed ledger technology, however, may be used in the clearance and settlement of digital assets and may not lend itself to traditional clearance and settlement regulation, which is focused on centralized providers of clearance and settlement services.

Lending, Borrowing, and Collateral

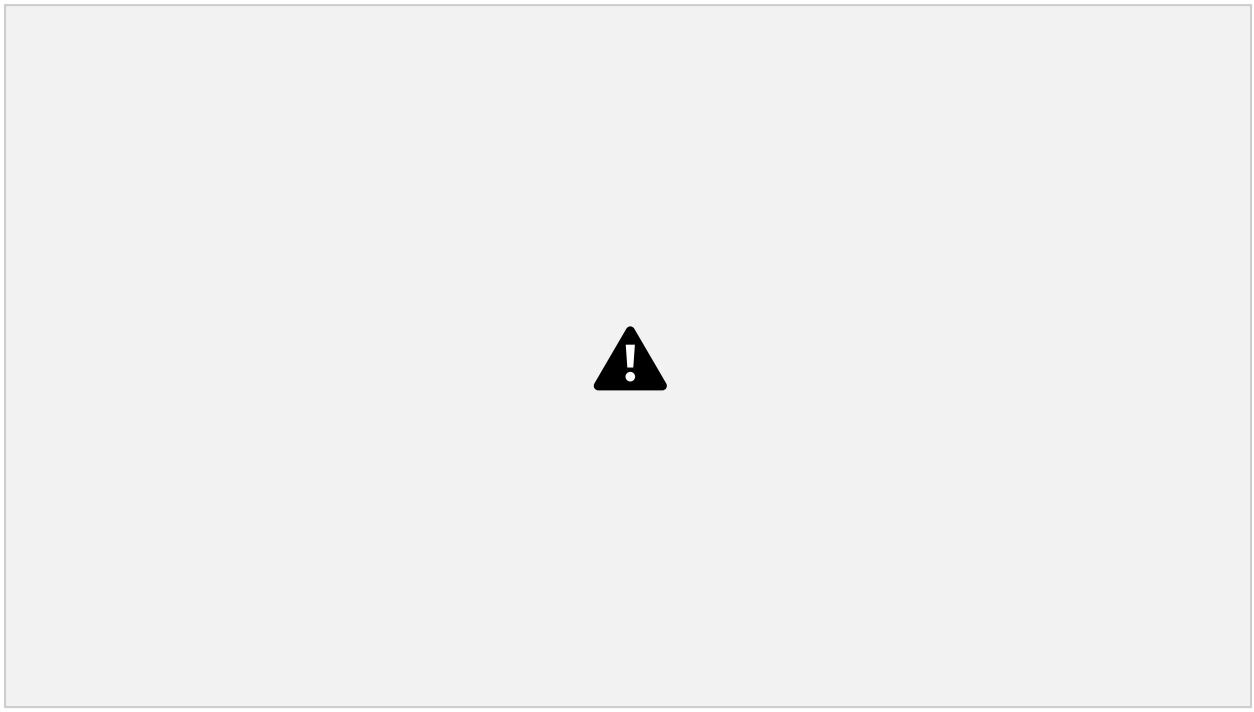
Prime brokers operate in the digital asset space as a way for institutional traders, including digital asset native funds, to obtain leverage. Currently, the prime brokerage space for digital assets in the United States is

nascent, potentially due to earlier regulatory regimes. Prime brokers offer financing, custody, and order routing

107 *See* 17 C.F.R. § 240.15c3-3 (2024).
108 *See* 15 U.S.C. § 78ccc et seq.
109 To date, given the lack of clear regulatory guidance surrounding digital assets, the appropriate safeguarding of digital asset securities through intermediaries like broker-dealers has remained challenged.
110 *See*, *e.g.*, Section 4d(2) of the CEA (7 U.S.C. § 6d(2)); 17 C.F.R. § 1.20 (2024).
111 *See, e.g.*, 31 U.S.C. §§ 5312(a)(2)(G), (H); 31 C.F.R. §§ 1010.100(h), (x) (2024); 31 C.F.R. § 1023.210 (2024); 31 C.F.R. § 1026.210 (2024); *see also* Heath Tarbert, Kenneth A. Blanco & Jay Clayton, Leaders of CFTC, FinCEN, and SEC Issue Joint Statement on Activities Involving Digital Assets (Oct. 11, 2019), https://www.fincen.gov/sites/default/files/2019-10/CVC%20Joint%20Policy%20Statement_508%20FINAL_0.pdf.
112 15 U.S.C. § 78q-1.
113 *See* 17 C.F.R. § 240.17ad 22(a) (2024).
114 15 U.S.C. § 78mm.

solutions across digital asset-linked derivatives and securities (e.g., futures and ETPs).[115] In addition, borrowing against one's digital asset holdings, primarily bitcoin, has been popular among retail investors. DeFi also provides opportunities to borrow against digital assets as collateral. While DeFi lending has focused on retail investors, DeFi protocols have recently been established to allow institutional investors to borrow against their digital assets.[116]

Trends in Crypto Lending[117]



Commercial Applications

The activities described above, notably trading, constitute the majority of financial market applications involving digital assets. Nevertheless, a significant number of consumer applications have employed blockchain technology to record ownership and allow users to engage in several different types of non financial activities.[118] For example, tokens may provide a "utility," such as the ability to access, transact, or interact with goods and services within a particular blockchain network or application.[119] Alternatively, they may grant a holder rights to participate in a pre-defined activity, such as attending a concert or other event. Other types of digital asset tokens may provide a holder with ownership of value derived offchain, distinct from any value derived from the blockchain itself—such as art, collectibles, memberships, and other tangible and

intangible goods.

115 In CFTC-regulated markets, prime brokerage services are provided by FCMs, which must be registered with the CFTC in order to offer access to derivatives on digital asset commodities to their customers. *See* National Futures Association, *Futures Commission Merchant (FCM) Registration,* https:// www.nfa.futures.org/registration-membership/who-has-to-register/fcm.html (last visited July 13, 2025).

116 *See, e.g.*, *The Elevator Pitch*, Wildcat Protocol Documentation, https://docs.wildcat.finance/overview/introduction.

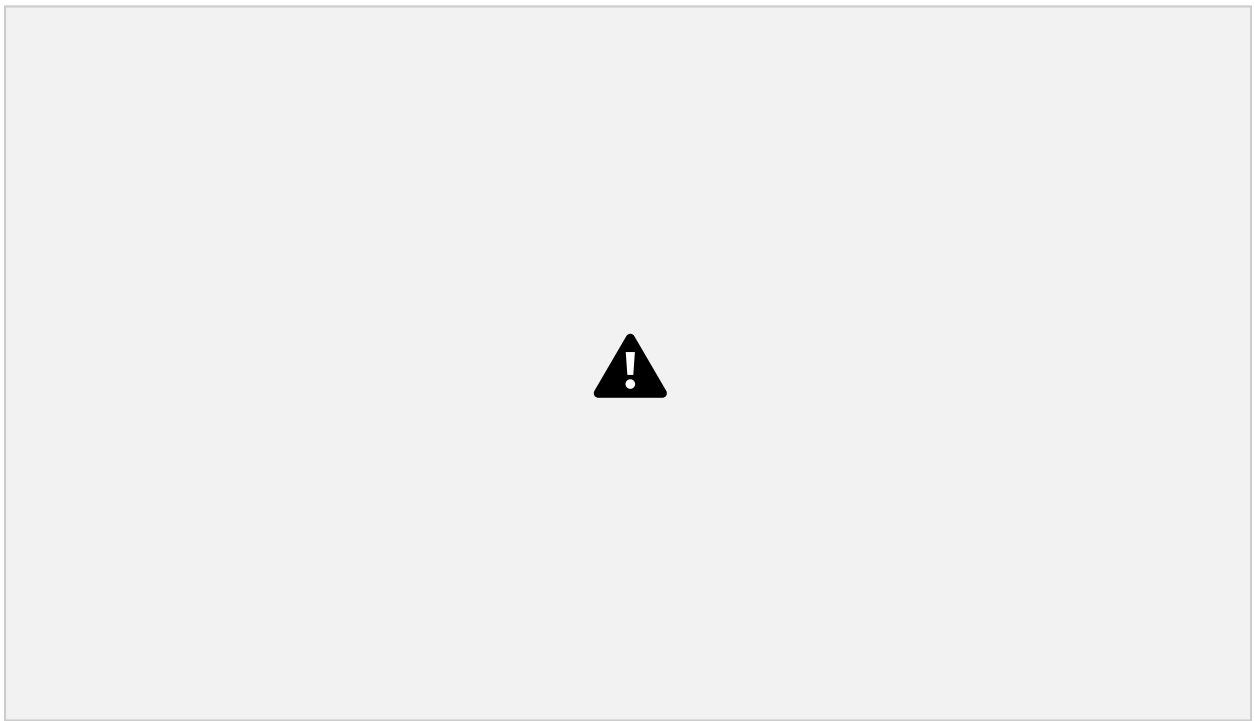
117 Zack Pokorny, *The State of Crypto Leverage – Q1 202*5, Galaxy (June 4, 2025), https://www.galaxy.com/insights/research/the-state-of-crypto-leverage-q1-2025. 118 *See Blockchain Use Cases*, Consensys, https://consensys.io/blockchain-use-cases (last visited July 13, 2025); *The State of Crypto: The Future of Money Is Here Report*, Coinbase (Jun. 10, 2025), https://www.coinbase.com/blog/the-state-of-crypto-the-future-of-money-is-here.

119 Corey Barchat, *What are utility tokens and how do they work?*, Moonpay (Aug. 6, 2024), https://www.moonpay.com/learn/cryptocurrency/what-are-utility-tokens.

Tokenization

Tokenization refers to the practice of using blockchain technology to record ownership of an asset. These assets can take the form of traditional financial assets, such as money market fund shares or bank deposits, or non-financial assets, such as trade receivables or interests in rare items such as art or collectibles. Industry estimates suggest that over $600 billion in “real world assets” could be tokenized by 2030.[120]

Market Size of Tokenized Real World Assets[121]



Similarto the benefits that arose from the electronification of financial markets decades ago, which involved the dematerialization of securities,tokenization can enable new financial products by dematerializing and mobilizing them through smart contracts and other blockchain-based technologies.[122]

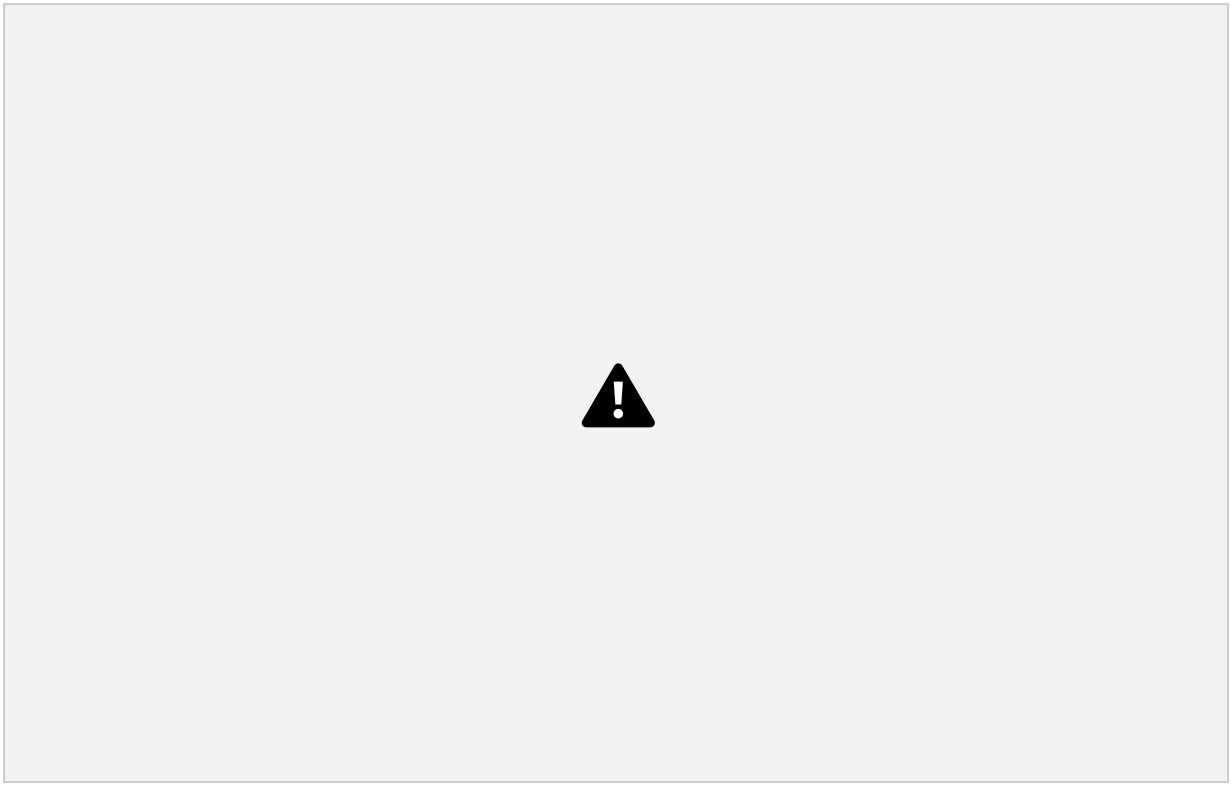
Firms are increasingly tokenizing money market fund shares, fixed-income products, private fund shares, and private credit.[123] The CFTC has noted the potential for tokenization to improve the collateral market with atomic settlement[124] and ameliorate liquidity needs in bilateral and multilateral clearing.[125]

Several other benefits of tokenization include the programmability and peer-to-peer transferability

120 David Chan et al., Tokenized Funds: The Third Revolution in Asset Management Decoded, Boston Consulting Group, Aptos Ascend & Invesco (Oct. 2024), https://web-assets.bcg.com/81/71/6ff0849641a58706581b5a77113f/tokenized-funds-the-third-revolution-in-asset-management-decoded.pdf. 121 Graphic provided by Plume. The chart starts at September 2021—the month the Ethereum community officially recognized the ERC3643 tokenization protocol as an official standard for permissioned tokens. *See ERC3643: An Official Standard for Permissioned Tokens*, Tokeny (Sept. 23, 2021), https://tokeny.com/erc3643-an-official-standard-for-permissioned-tokens.
122 *See Is Tokenization Bringing Wall Street On-Chain?*, 21shares (Feb. 11, 2025), https://www.21shares.com/en-us/research/newsletter-issue-260. 123 *See e.g.,* Sandy Kaul, *Tokenized Money Market Funds: The Bridge to a New Financial Infrastructure*, Franklin Templeton (Jun. 9, 2025), https://www.franklintempleton.co.uk/articles/2025/disruption/tokenized-money-market-funds-the-bridge-to-a-new-financial-infrastructure. 124 For a discussion ofthe benefits of atomic settlementin financial markets, *see* Michael Lee, Antoine Martin, & Benjamin Muller, *What is Atomic Settlement,* Federal Reserve Bank of New York: Liberty Street Economics (Nov. 7, 2022), https://libertystreeteconomics.newyorkfed.org/2022/11/what-is-atomic-settlement. 125 Press Release, CFTC, *CFTC's Global Markets Advisory Committee Advances Recommendation on Tokenized Non-Cash Collateral* (Nov. 21, 2024), https://www.cftc.gov/PressRoom/PressReleases/9009-24.

of assets, operational efficiencies (e.g., 24/7 trading and simplified recordkeeping), and increased transparency relative to traditional financial markets.

Tokenization Process[126]



Currently, the tokenization landscape is comprised by firms operating tokenized platforms solely through private, permissioned blockchains and those deploying permissioned systems on top of public, permissionless blockchains.

The regulatory structure of tokenization is determined by what asset is tokenized, not the mere process of tokenizing an asset.[127] Where tokenized instruments have been regulated, they tend to be regulated as securities, as much of the current volume in tokenization falls with underlying assets that are securities (e.g., fixed income and private credit). Additional non-security uses of tokenization include tokenized commodities (e.g., gold) and tokenized non-financial assets (e.g., commercial real estate and rare items[128]).

126 Graphic prepared by Ondo Finance.
127 *See* Commissioner Hester M. Peirce, SEC, *Enchanting, but Not Magical: A Statement on the Tokenization of Securities* (July 9, 2025), https://www.sec.gov/newsroom/speeches-statements/peirce-statement-tokenized-securities-070925 ("As powerful as blockchain technology is, it does not have magical abilities to transform the nature of the underlying asset.").
128 *See, e.g.*, Jay Speakman & Paolo Besabella, *Revolutionizing the Art World: An In-Depth Look at Art Tokenization*, BeInCrypto (Dec. 31, 2022), https://beincrypto.com/what-is-art-tokenization.

Potential Risks to Consumers and Market Participants

Americans who choose to use digital assets for their financial services needs, such as to make payments, trade, and invest, may benefit from lower costs, faster payments, and more seamless portability of services. However, they also face risks similar to those arising from traditional financial products and services. The lack of regulatory certainty has obscured these risks and made it more difficult to discern applicable regulatory protections.

Custody Risks

Many individuals and institutions use intermediaries for buying, selling, trading, and storing digital assets. These intermediaries offer products and services such as crypto ATMs, custody arrangements, trading platforms, and ETFs. However, reliance on intermediaries can introduce risks related to bankruptcy, market manipulation, conflicts of interest, data privacy, cybersecurity, theft, and fraud.

Non-custodial wallets—through which parties may exercise individual control over their digital assets—eliminates intermediary risks and increases privacy. Non-custodial cold wallets are not connected to the internet and therefore reduce cyberattack risks. However, non-custodial wallets require individuals to manage their private keys. Loss or theft of a private key generally results in the loss of digital assets.

Fraud and Cybersecurity Risks

Similar to traditional markets, digital asset markets face risks from fraud, manipulation, and illicit conduct. Weak controls by intermediaries can lead to unauthorized transfers and stolen credentials. Smart contracts may also introduce certain risks due to potential coding errors, inadequate testing or auditing of code, or security vulnerabilities that can be exploited, leading to unauthorized transfers or loss of funds.

Data Privacy Risks

In public blockchain networks, transaction and ownership information is often public or shared, potentially revealing identities via metadata despite being pseudonymous. This is especially concerning for payments, as transaction details can infer or reveal personal identifying information, like residence and demographics. Using self-custody and privacy-enhancing technologies can reduce privacy risks. At times, however, users may not be able to remain truly pseudonymous to all actors. For example, financial intermediaries are required by law, including requirements under the BSA, to collect and maintain certain information about the identity of transaction participants.

Operational Risks

Investors and consumers face operational risks from flawed processes, system failures, human errors, governance lapses, data breaches, and other external disruptions. These can include information system deficiencies, processing delays, system outages, and security threats. The manner in which blockchains operate comes with challenges, including irreversible transactions and network interoperability issues. Smart contracts, while efficient, may include coding errors and security flaws, leading to unauthorized transfers or loss of funds. Resolving these issues is difficult due to transaction immutability and limited legal recourse.

Cryptocurrency and the Technical Standards Landscape

The Role of Technical Standards and NIST

Technical standards are specifications for a product, process, or service designed to ensure quality and interoperability across businesses and national boundaries. By giving every market participant the same guidance, standards reduce barriers to trade, shorten time-to-market, and increase consumer confidence through safety and reliability assurances.

Technical standards are issued by standards development organizations (SDOs), ranging from industry groups to international nonprofits, and often feature multi-stakeholder processes. In the United States, the National Institute for Standards and Technology (NIST)—within the Department of Commerce— leads governmental efforts in standards development through two main pathways:

1. Pre-Standardization Research: NIST conducts research and publishes technical whitepapers, guidelines, and frameworks that serve as a foundation for future standards, such as NIST's widely adopted Cybersecurity Framework 2.0. When developing these contributions, NIST uses an open and transparent process that encourages participation from industry and academic networks.
2. Representing Industry and National Interests in SDOs: Industry has several avenues for participating in international standard-setting processes, butthose processes can be resource intensive and prohibitively complex for smaller companies. NIST is an active participantin international standard setting, providing impartial technical expertise and ensuring that *all* U.S. industry voices, from the multinational corporation to the small entrepreneur, are reflected in final standards.

Through these pathways, NIST support the United States' industry-led, market-driven, and voluntary approach to international standards development. The standards NIST facilitates can substitute for regulation, provide an ideal environment for innovation, and ensure that industry norms reflect decentralized input.

Technical Standards and Digital Assets

The digital asset ecosystem should harness the power of standards to solve coordination problems without government intervention. Technical standards are already relevant to the digital asset

ecosystem. Various international organizations—including the Institute of Electrical and Electronics Engineers (IEEE), the International Organization for Standardization (ISO), the International Electrotechnical Commission (IEC), the World Wide Web Consortium (W3C), the Internet Research Task Force, and the Internet Engineering Task Force—have released or are developing technical standards relevant to Distributed Ledger Technologies (DLTs). The ISO, IEEE and W3C in particular have played important roles in standardizing smart contracts and addressing within DLT systems, such as through ISO 23455:2019 or IEEE P3207.

Technical Standards and Post-Quantum Cryptography

The modern financial system is built on cryptography, and digital assets are no exception. As discussed in *Chapter I, Crypto 101*, digital assets live at addresses on blockchains. Users controlthese addresses like accounts and digitally sign transactions to prove authenticity when sending assets to another address.

Blockchains implement these digital signatures through public-key cryptography. In this set-up, a user signs using a private key, which is kept hidden, butreleases a public key, which lets other users verify their signature as authentic. These public-private key pairs undergird the functionality of blockchains.

If someone obtains a user's private key, or otherwise derives it,the new holder ofthe private key can fraudulently transfer and stealthe user's assets. The foundation for modern public-key implementations is that it is computationally intractable for conventional computers to deduce a user's private key from the public key, keeping digital assets secure.

Quantum computing would jeopardize that security. Quantum computers exploit quantum mechanical phenomena to solve mathematical problems that are difficult or intractable for modern computers. That includes the problem of deriving a private key from a public key. Such a development would fundamentally threaten *all* encrypted financial transactions, from bank transfers to credit card payments to blockchains.

For digital assets in particular, anyone with a quantum computer of sufficient strength could derive *any* digital-asset holder's private key from their public key and steal all of the user's digital assets, potentially leading to widespread digital asset theft.[129] While current quantum computers are far from powerful enough to break cryptographic keys, some experts estimate that cryptographically relevant quantum computers could emerge in the next five to ten years.[130]

Cryptographers have not stood idly by in the face of this threat. To replace existing encryption algorithms, they have searched for mathematical problems that even quantum computers cannot solve efficiently. This has resulted in several post-quantum cryptographic algorithms.

In 2016, NIST launched the post-quantum cryptography (PQC) standardization project to solicit, evaluate, and standardize one or more of these algorithms to replace current cryptographic standards. The goal was to develop a standard cryptographic system secure against quantum that could interoperate with existing communications protocols and networks.

In August 2024, NIST finalized its principal set of post-quantum encryption algorithms:

- *Federal Information Processing Standards (FIPS) 203:* Module-Lattice-Based Key-Encapsulation Mechanism Standard.

- *FIPS 204:* Module-Lattice-Based Digital Signature Standard.
- *FIPS 205:* Stateless Hash-Based Digital Signature Standard.

To defend against quantum threats,PQC will need to be adopted across the digital asset ecosystem *before* a cryptographically relevant quantum computer is developed. Private actors should implement PQC where practical, while working to identify and address cases where it will be more challenging to deploy.

The transition to post-quantum cryptography represents a particularly large and urgent shift in the implementation and use of cryptography, requiring the adoption and deployment of new cryptographic algorithms and technologies across our digital infrastructure at a scale and schedule never before envisioned. This will require flexible and agile approaches for building, maintaining, and operating systems that use cryptography.

129 The Bitcoin protocol encourages users to change their public keys regularly, mitigating this vulnerability, yet roughly 25-33% of Bitcoin is still in wallets that have not changed their public keys at all. *See* Anthony Milton & Clara Shikhelman, *What Happens to Bitcoin When Quantum Computers Arrive?*, Bitcoin Magazine (June 20, 2025), https://bitcoinmagazine.com/technical/what-happens-to-bitcoin-when-quantum-computers-arrive; Itan Barmes, Bram Bosch & Olaf Haalstra, *Quantum computers and the Bitcoin blockchain*, Deloitte (Jan. 7, 2025), https://www.deloitte.com/nl/en/services/risk-advisory/perspectives/quantum-computers-and-the-bitcoin-blockchain.html; Itan Barmes et al., *Quantum risk to the Ethereum blockchain - a bump in the road or a brick wall?*, Deloitte (Feb. 2022), https://www.deloitte.com/nl/en/services/risk-advisory/perspectives/quantum-risk-to-the-ethereum-blockchain.html (The Ethereum protocol assumes that users will reuse the same public key, making over 65% of all Ether currently vulnerable according to some estimates).

130 *See* Michele Mosca & Marco Piani, *Quantum Threat Timeline Report 2024*, Global Risk Institute (Dec. 2024), https://globalriskinstitute.org/publication/2024- quantum-threat-timeline-report.

Cryptographic agility (sometimes referred to as "crypto agility") refers to a platform's capacity to seamlessly replace cryptographic algorithms without disrupting operations or compromising security. Cryptographic agility helps organizations:

- Integrate and deploy PQC algorithms alongside or in place of classical algorithms.
- Manage long and complex migration periods while maintaining compatibility.
- Swap out weak or deprecated algorithms quickly in response to new vulnerabilities.
- Reduce the operational and technical cost of cryptographic transitions.

Distributed ledgers face unique challenges in becoming cryptographically agile. Permissionless blockchains require consensus among thousands of nodes, with no central authority to coordinate updates.[131] Additionally, the immutable nature of blockchains means that all past transactions will have to remain valid even after transitioning to a new cryptographic scheme, and preserving the integrity of decades of past data requires complex mechanisms.[132]

Advancing American Leadership Through Technical Standards

The United States should lead the way in laying a foundation for further digital asset standards through its pre-standardization research and industry representation. In the absence of U.S. leadership in shaping and promoting widely adopted standards, the development of cryptocurrencies and post-quantum upgrades may face both technical and strategic limitations.

The current technical standards underpinning the digital asset landscape are fragmented, and thus inhibit the maturation and adoption of the broader crypto industry. Existing SDO standards can be limited in scope, offering common definitions and frameworks but falling short of universally accepted guidance that is necessary to establish interoperability within the crypto ecosystem. Many project foundations have developed their own protocols for DLTs—advancing the technical frontier but

leaving unaddressed key technical questions that would enable interoperability, cybersecurity, privacy, and stability for all. NIST can play an essential role in facilitating industry adoption of common practices to address these challenges.

NIST has already begun taking initial steps to support the DLT ecosystem. It has published technical reports providing fundamental overviews of relevant technologies, as well as more specific information on cybersecurity considerations, such as NIST IR 8403, *Blockchain for Access Control Systems*. Further technical guidelines, covering areas such as wallet security, cross-chain bridge protocols, and incident response procedures, would promote wider adoption of cybersecurity and interoperability best practices across the industry.

Strategically, U.S. leadership in technical standards is not just helpful for industry growth—it is vital for advancing the national interest. If the United States does not lead in standard-setting practices for the crypto industry, the development of this technology will proceed outside our borders. This could result in standards that advantage foreign competitors over U.S. companies or conflict with American values. Sustained U.S. leadership—grounded in NIST's technical rigor and active engagement in global standard-setting—can ensure that the next generation of digital-asset infrastructure both closes today's gaps and advances national interests.

131 Shin'ichiro Matsuo et al., Presentation at NIST Crypto Agility Workshop, Crypto-Agility for Blockchain Protocol: The Difference Compared to Existing Crypto-Agility Concepts, Transition Mechanisms, and Issues Specific to Blockchain Protocols (Apr. 18, 2025), https://csrc.nist.gov/csrc/media/Events/2025/ crypto-agility-workshop/documents/presentations/s8-kigen-fukuda-presentation.pdf.

132 *Id.*

CHAPTER III

Digital Asset Market Structure

Digital Asset Market Structure

> When there's enough scale, maybe there can be an exchange site that doesn't do transfers, just matches up buyers and sellers to exchange with each other directly . . . To make it safer, the exchange site could act as an escrow for the bitcoin side of the payment. The seller puts the bitcoin payment in escrow, and the buyer sends the conventional payment directly to the seller. The exchange service doesn't handle any real world money.
>
> BitcoinTalk Forum Post re: "Money Transfer Regulations"
> Satoshi Nakamoto, March 2010[133]

> Bitcoins have no dividend or potential future dividend, therefore not like a stock. More like a collectible or a commodity.
>
> BitcoinTalk Forum Post re: "Bitcoins are most like shares of common stock"
> Satoshi Nakamoto, August 2010[134]

Satoshi was prescient in his vision of an "exchange site." Before centralized or decentralized exchanges came into the fold, transactions between market participants were peer-to-peer in the purest form—trades arranged on the BitcoinTalk forum or meetups organized on LocalBitcoins.com.[135] Mt. Gox, originally a trading card marketplace that emerged as the dominant centralized exchange for bitcoin by 2013,[136] famously collapsed in 2014 after a series of thefts resulting from inadequate cybersecurity and storage of its private keys.[137] What many thought to be the end of bitcoin, and digital assets broadly, instead spurred the

development of hundreds of trading platforms and digital asset service providers over the next decade.

This rapid growth, in size and scope, was not powered solely by retail traders hoping for their next "moonshot."[138] Capital across the globe flowed into the space because blockchain technologies could fundamentally transform financial systems, challenge traditional business models, redefine concepts of governance and ownership, and much more. Many innovations, such as tokenization, can introduce efficiencies into existing financial services like lending, trading, insurance, and capital formation. Fortunately, for the United States and the world, many years of innovation lie ahead.

To ensure this innovation, financial and otherwise, takes place in the United States, American markets for digital assets need to become the deepest and most liquid in the world. Just as the United States is the premier destination for capital markets activity—due in part to the well-established regulatory framework for traditional markets—it is imperative that the United States lead by establishing clear rules for digital asset markets.

133 satoshi, Comment to *Re: Money Transfer Regulations*, BitcoinTalk (Mar. 3, 2010 at 4:28 AM), https://bitcointalk.org/index.php?topic=69.msg614#msg614.
134 satoshi, Comment to *Re: Bitcoins are most like shares of common stock*, BitcoinTalk (Aug. 27, 2010 at 4:39 PM), https://bitcointalk.org/index.php?topic=845.msg11403#msg11403.
135 *See The Early Days of Crypto Exchanges*, Gemini, https://www.gemini.com/cryptopedia/crypto-exchanges-early-mt-gox-hack (updated Feb. 26, 2025); Jeff John Roberts, *The LocalBitcoins Era of Crypto Is Over, but Its Spirit Lives On,* Fortune: Crypto (Feb. 13, 2023 9:53 AM EST), https://fortune.com/ crypto/2023/02/13/the-localbitcoins-era-of-crypto-is-over-but-its-spirit-lives-on.
136 Takashi Mochizuki, Kathy Chu & Eleanor Warnock, *Tracing a Bitcoin's Exchange's Fall From the Top to Shutdown*, The Wall Street Journal (Apr. 20, 2014 at 7:10 PM ET), https://www.wsj.com/articles/SB10001424052702304311204579508300513992292.
137 *See* Jeremy Wagstaff, *Mt. Gox Bitcoin Debacle: Huge Heist or Sloppy Glitch?*, Reuters, https://www.reuters.com/article/technology/mt-gox-bitcoin-debacle huge-heist-or-sloppy-glitch-idUSL3N0LX2SP (updated Feb. 28, 2014).
138 The term "moonshot," derived from the phrase "to the moon," is used by cryptocurrency enthusiasts to express the expectation of a rapid increase in value. *See To the Moon Meaning*, Ledger Academy: Crypto Glossary, https://www.ledger.com/academy/glossary/to-the-moon (updated Oct. 4, 2023).

Much of this starts with the federal market regulators. Both the SEC and CFTC have taken strong initial steps since President Trump's inauguration to provide long-needed clarity to market participants.

- Ended the Biden-era SEC's enforcement first approach that disproportionately targeted disfavored industries.
- Established a Crypto Task Force under Commissioner Peirce's leadership, which solicited broad public input, held over one hundred meetings with market participants, and conducted five public roundtables.
- Rescinded SAB No. 121 (a staff bulletin that created significant regulatory burdens for companies that provide digital asset custody services).
- Provided staff-level clarity on the security status of memecoins, stablecoins, and mining and staking activities.
- Issued staff-level clarity on disclosure requirements for crypto-related offerings and registrations.
- Withdrew, together with FINRA, the unduly restrictive joint staff statement on broker dealer custody of digital asset securities.
- Published staff-level FAQs providing clarity on broker-dealer financial responsibility and transfer agent issues.
- Abandoned the Biden-era SEC's rule proposals related to crypto, including proposed rules to further define the statutory term "exchange" and proposed safeguarding rules.

- Ended regulation-by-enforcement and refocused the Division of Enforcement on fraud and helping victims.
- Hosted a first-ever Crypto CEO Forum of industry-leading firms on digital asset market structure.
- Acted on recommendations of CFTC's Digital Asset Markets Subcommittee (DAMS) of the Global Markets Advisory Committee (GMAC) on U.S. digital asset taxonomy and tokenized non-cash collateral.
- Committed to participate as an observer in industry tokenization initiatives.
- Launched two significant digital asset market structure innovations that are currently active on CFTC DCMs, perpetual derivatives and 24/7 trading hours, and requested public comment.
- Issued staff-level clarity on cross-border definitions for U.S. location and U.S. persons for both futures and swaps activity, including crypto exchanges, trading firms, and other market participants.
- Withdrew two outdated staff-level advisories relating to virtual currency derivative product listings and clearing that were unduly restrictive given digital asset market growth and maturity.

Despite the progress that both regulators have made, much work remains to be done. An express goal of the Trump Administration is to reduce unnecessary regulations, avoid new burdensome regulations, and promote U.S. leadership in the digital asset space. The Working Group supports regulatory efforts to facilitate trading and custody of digital assets on venues regulated at the Federal level in short order. Toward that end, it is necessary to understand the regulatory frameworks the SEC and CFTC apply to markets for digital assets and align on an appropriate taxonomy.

Establishing a Taxonomy for Digital Assets

U.S. regulatory agencies have attempted to classify digital assets under existing frameworks. For example, the CFTC recognized that bitcoin and ether are commodities, while the SEC has treated other digital assets as securities based on their structures, methods of distribution, and uses.[139] Yet, without a clear and comprehensive classification system, market participants have had to navigate a patchwork of interpretations and guidance—a proverbial minefield for honest actors trying to lead the industry forward. A clearer, agreed upon taxonomy is essential to ensure both the healthy development of the digital asset ecosystem and consumer and investor protection.[140]

As the economic functions of digital assets vary, the appropriate federal regulator for digital asset markets— when there is one—should generally depend on such digital assets' functions. Below we discuss segmenting the asset class into three categories—security tokens, commodity tokens, and tokens for commercial and consumer use.

Security Tokens

Certain digital assets may constitute securities (such as those that represent an interest in equities, bonds, or security-based swaps, among other products) or be offered and sold as part of a type of security called an "investment contract," such that the transactions constitute securities subject to the federal securities laws.

Pursuant to Section 5 of the Securities Act of 1933 (Securities Act),[141] any offer and sale (including any resale) of a security involving a digital asset must be made by filing a registration statement under the Securities Act with the SEC or be conducted pursuant to an available exemption from registration under the Securities Act. The issuer of a security involving a digital asset may become subject to the periodic and current reporting
requirements of the Securities Exchange Act of 1934 (Exchange Act).[142] As a result, issuers file certain reports with the SEC, including annual, periodic, and current reports.

Pursuant to Section 2(a)(1) of the Securities Act and Section 3(a)(10) of the Exchange Act, a security includes a "stock," "note," "evidence of indebtedness," and "an investment contract," among other categories.[143] In 1946, the U.S. Supreme Court, in *SEC v. W.J. Howey Co.*, defined an investment contract as an "investment of money in a common enterprise with profits to come solely from the efforts of others."[144] This definition embodies a "flexible rather than a static principle, one that is capable of adaptation to meet the countless and variable schemes devised by those who seek the use of the money of others on the promise of profits."[145] The SEC continues to use the U.S. Supreme Court's "*Howey* Test" to analyze whether a contract, transaction, or scheme is an "investment contract."[146]

139 While bitcoin and other virtual currencies are not explicitly defined as commodities under Section 1a(9) of the Commodity Exchange Act, the CFTC acknowledged in a 2015 settlement order that the definition of a "commodity" is broad and encompasses Bitcoin and virtual currencies. *See* Commodity Futures Trading Commission, Order: Coinflip, Inc., d/b/a Derivabit, et al. (Sept. 17, 2015). This position was upheld by a U.S. District Court decision in 2018. *CFTC v. McDonnell*, 287 F. Supp. 3d 213, 217 (E.D.N.Y. 2018).

140 There is a similar need for clarity as to how digital assets are classified for Federal income tax purposes. Multiple provisions of the Internal Revenue Code apply only to assets treated as securities for tax purposes, or only to assets treated as commodities for tax purposes, or apply differently to securities and to commodities. Under current law, the tax classification of financial instruments as securities or commodities is not necessarily the same as the regulatory classification, so that regulatory clarity will not necessarily bring comparable tax clarity. For further discussion of this issue, *see Chapter VII*.

141 15 U.S.C. § 77e.

142 15 U.S.C. § 78m and *o*.

143 *See* 15 U.S.C. §§ 77b-77c.

144 328 U.S. 293, 301 (1946); *See SEC v. Edwards*, 540 U.S. 389, 393 (2004); *see also United Hous. Found., Inc. v. Forman*, 421 U.S. 837, 852-53 (1975) (The "touchstone" of an investment contract "is the presence of an investment in a common venture premised on a reasonable expectation of profits to be derived from the entrepreneurial or managerial efforts of others.").

145 *W.J. Howey Co.*, 328 U.S. at 299.

146 *See, e.g.*, *SEC v. Barton*, 135 F.4th 206, 215-217 (5th Cir. 2025).

A digital asset that is a note or debt instrument[147] presumptively is a security.[148] This presumption may be rebutted through the "family resemblance test" by showing the note strongly resembles one of several types of notes that is issued in connection with typical commercial transactions and, accordingly, is excepted from the definition of security.[149]

Any platform that operates as an "exchange" as defined under Section 3(a)(1) of the Exchange Act[150] and Rule 3b-16(a) thereunder for digital assets that are securities must register as a national securities exchange or operate pursuant to an exemption in conjunction with the SEC's relevant exemptive authority. An entity that meets the definition of an "exchange" may rely on the exemption from registration for an alternative trading system (ATS). An ATS is exempt under Exchange Act Rule 3a1-1(a)(2)[151] from registration as a national securities exchange pursuant to Sections 5 and 6 of the Exchange Act if the ATS complies with applicable conditions in Regulation ATS.[152] The conditions of Regulation ATS include, among other things, the ATS registering as a broker-dealer and filing disclosures with the SEC.

Any intermediaries acting as a "broker"[153] or "dealer"[154] in digital assets that are securities in interstate commerce are required to register with the SEC and are subject to SEC oversight.[155] Traditionally, broker dealers maintain customer accounts and exercise certain levels of control over customer assets through custodial arrangements. Absent an exemption,[156] such intermediaries also are required to become members of FINRA and are subject to FINRA oversight.[157] As a self-regulatory organization, FINRA writes and enforces its own rules for member firms subject to federal securities laws and is also subject to SEC oversight.[158]

Market participants who use broker-dealers registered with the SEC to custody their securities (and related cash) benefitfrom the protections provided by the federal securities laws, including the customer protection rule[159] and, in most cases, the Securities Investor Protection Act of 1970 (SIPA).[160] Any SEC-regulated entities that are defined as "financial institutions" are subjectto requirements underthe Bank Secrecy Act, including anti-money laundering (AML) program requirements.[161] As a result, broker-dealers and mutual funds, among otherregistered entities, are required to implementreasonably-designed AML programs and report suspicious activity.

A host of additional activities within the lifecycle of a digital asset that is a security may invoke federal securities laws. Pursuant to the Exchange Act[162] any entities acting as a "transfer agent"[163] with respect to certain

147 For more information on notes and debt instruments, *see Debt Security*, Westlaw Practical Law (2025).

148 *Reves v. Ernst & Young*, 494 U.S. 56, 64-66 (1990). Federal courts apply the *Reves* test to notes as well as to other instruments with debt characteristics. *See, e.g.*, *In re Tucker Freight Lines, Inc*., 789 F. Supp. 884, 885 (W.D. Mich. 1991).

149 *See, e.g.*, *SEC v. Thompson*, 732 F3d 1151, 1169-1161 (10th Cir. 2013).

150 Section 3(a)(1) of the Exchange Act defines an "exchange" as "any organization, association, or group of persons, whether incorporated or unincorporated, which constitutes, maintains, or provides a marketplace or facilities for bringing together purchasers and sellers of securities or for otherwise performing with respect to securities the functions commonly performed by a stock exchange as that term is generally understood, and includes the market place and the market facilities maintained by such exchange."

151 17 C.F.R. § 240.3a1-1(a)(2) (2024).

152 An ATS that fails to comply with the requirements of Regulation ATS would no longer qualify for the exemption provided under Exchange Act Rule 3a1-1(a)(2), and thus, risks operating as an unregistered exchange in violation of Section 5 of the Exchange Act. 15 U.S.C. § 77e.

153 Section 3(a)(4) ofthe Exchange Act defines a "broker" as "any person engaged in the business of effecting transactions in securities forthe account of others." 154 Section 3(a)(5) of the Exchange Act defines a "dealer" as "any person engaged in the business of buying and selling securities … for such person's own account through a broker or otherwise."

155 15 U.S.C. § 78o(a)(1).

156 *See* Exchange Act Rule 15b9-1 (exempting broker-dealers from securities association membership if they are a member of a national securities exchange, carry no customer accounts, and effect transactions in securities that are solely offered through the national securities exchange to which it is a member). 157 15 U.S.C. § 78o(b)(8).

158 *See, e.g.*, *Crypto Assets: Overview*, FINRA https://www.finra.org/rules-guidance/key-topics/crypto-assets (last visited July 13, 2025). 159 *See* Exchange Act Rule 15c3-3.

160 *See* 15 U.S.C. § 78ccc et seq.

161 31 U.S.C. § 5311 et seq.

162 15 U.S.C. § 78q-1.
163 As defined by Section 3(a)(25) of the Exchange Act.

securities that are digital assets are required to register with the SEC. Registered transfer agents maintain the record of ownership of the issuer's securities and provide certain shareholder services. Similarly, Section 17A of the Exchange Act and Rule 17Ab2-1 thereunder, subject to certain exemptions and exclusions, require an entity to register with the SEC prior to performing the functions of a "clearing agency,"[164] which include serving as a central counterparty (CCP) or a central securities depository (CSD).[165]

In addition, the SEC regulates or subjects to reporting obligations a variety of institutional investors. These include registered investment companies and private funds (e.g., venture capital funds, hedge funds, and private equity funds). The Investment Company Act of 1940 (Investment Company Act)[166] requires pooled investment vehicles primarily investing in securities that are not excepted or exempted to register with the SEC. Investment companies publicly offer and sell their securities, may tokenize their own securities, and may invest in digital assets that are securities as well as other types of digital assets.

The Investment Advisers Act of 1940 (Advisers Act)[167] requires persons that manage the portfolios of registered investment companies to register as an "investment adviser" with the SEC and, depending on the amount of assets under management, requires other persons who engage in the business of advising others as to the advisability of investing in, purchasing, or selling securities to register with the SEC, absent an exemption. Pursuant to Advisers Act Rule 206(4)-2,[168] registered investment advisers who have custody of client funds or securities must comply with an enumerated set of requirements to prevent loss, theft, misuse, or misappropriation of such client assets, including using a "qualified custodian" as defined under the rule.

Tokenized Securities

Companies are increasingly using blockchain technology or other distributed ledger technology to record the ownership of securities that they issue by representing the securities as digital assets on a blockchain or other DLT network (i.e., tokenized securities). Tokenization does not affect the substance of the securities issued, nor does the use of a blockchain by an issuer or its agent give rise to a new or different type of asset.[169] Thus, tokenized securities fall squarely within the definition of "security" under the federal securities laws, and all offers and sales of such assets are subject to registration, absent an exemption.[170] Tokenization can enable investors to engage with and use the securities in new or enhanced ways through peer-to-peer and other blockchain-based transactions, including on or through DeFi protocols.[171]

The SEC has exemptive authority under existing federal securities laws that it can use to mitigate concerns related to the issuance and trading of tokenized securities. Section 36 of the Exchange Act provides the SEC with the authority to exempt any class of securities or transactions from requirements under the Exchange Act "to the extent that such exemption is necessary or appropriate in the public interest and is consistent with the protection of investors."[172] Section 28 of the Securities Act[173] provides the SEC with the authority to exempt any class of securities or transactions from requirements under the Securities Act "to the extent that such exemption is necessary or appropriate in the public interest and is consistent with the protection

164 As defined by Section 3(a)(23) of the Exchange Act.
165 *See* Exchange Act Rule 17Ad-22(a).
166 15 U.S.C. § 80a-51.
167 15 U.S.C. § 80b-20.
168 17 C.F.R. § 275.206(4)-2 (2024).
169 *See generally Division of Trading and Markets: Frequently Asked Questions Relating to Crypto Asset Activities and Distributed Ledger Technology*, Division of Trading and Markets of the SEC (May 15, 2025), https://www.sec.gov/rules-regulations/staff-guidance/trading-markets-frequently-asked-questions/frequently-asked-questions-relating-crypto-asset-activities-distributed-ledger-technology.
170 *See* Commissioner Peirce, *supra* note 127.
171 *See* Chapter II for a further discussion of Decentralized Finance protocols.
172 15 U.S.C. § 78mm.

173 15 U.S.C. § 77z-3.

of investors."[174] Using these authorities, the SEC, for example, could craft an exemptive framework to exempt persons seeking to operate a platform offering tokenized securities from certain existing federal securities laws and/or regulations. Such exemptive actions could be limited in time or scope.

Non-Security Digital Assets that are the Subject of an Investment Contract

Virtually any type of good, right, service, or interest can be represented as a digital asset on a blockchain or similar distributed ledger technology network. Although many digital assets are not securities, persons may distribute non-security digital assets as part of a contract, transaction, or scheme that satisfies each element of the "investment contract" definition under *SEC v. W.J. Howey Co*., and thus, as part of a security.[175] Digital assets, such as network tokens that are offered or sold as the subject of an investment contract, may be separable from the investment contract in some or all later transactions. Digital asset market participants, including issuers, trading venues, and early-stage purchasers face the resulting challenge of determining when a non-security digital asset subject to an investment contract separates from the investment contract.

As market participants attempt to deal with this issue with their own solutions, the SEC may consider using its existing authority to further address it. The SEC could provide both a tailored registration regime for certain digital asset securities and an appropriately conditioned "safe harbor" from securities registration for transactions involving digital assets that are (or might be) subject to an investment contract. Such a safe harbor would afford issuers time to progressively deliver functionality for a digital asset or decentralize a network or application, while providing material information to investors about the digital asset, the issuer, and its promised essential managerial efforts.

Digital Assets with the Intrinsic Characteristics of an Enumerated Type of Security Under the Federal Securities Laws

Depending on their intrinsic characteristics, certain digital assets may independently satisfy the definition of a "security" under the federal securities laws. For example, there may be certain hybrid or multi-use tokens with functionality that also contains the features of common stock, debt, or a derivative of a security (e.g. a security based swap). In this regard, the SEC may consider an assortment of potential solutions, which might include exemptive relief or other actions to address issues surrounding such hybrid or multi-use tokens.

Commodity Tokens

Many digital assets fall outside the definition of security and many of the laws that govern securities transactions. This subsection provides an overview of the market structure for non-security digital assets and the frameworks under which such assets could be regulated.

Certain digital assets may be commodities underlying a regulated derivatives transaction or may represent a derivative themselves (such as certain event contracts). The CFTC regulates such digital asset derivatives, subject to the Commodity Exchange Act (CEA). The CEA defines "commodity" broadly to include goods, services, articles, rights, and interests that are or could be the subject of futures contracts.[176] Bitcoin and ether, among other digital assets, have been recognized by federal courts and the CFTC as commodities within this definition.[177] When a digital asset meets the definition of a commodity, derivatives listed on that asset—including futures, options, and swaps—fall squarely within the CFTC's jurisdiction.

174 15 U.S.C. § 77z-3.
175 *See SEC v. Terraform Labs Pte. Ltd.*, 684 F. Supp. 3d 170, 194-201 (S.D.N.Y. 2023).

176 7 U.S.C. § 1a(9).
177 *See CFTC v. McDonnell*, 287 F. Supp. 3d 213, 228-29 (E.D.N.Y. 2018); *CFTC v. My Big Coin Pay, Inc*., 334 F. Supp. 3d 492, 496-97 (D. Mass 2018).

The CEA provides the CFTC with regulatory oversight of commodity derivatives and includes oversight for retail commodity transactions and retail foreign exchange transactions that are leveraged, margined, or financed. Currently, a listed derivative transaction requires the filing of a self-certification statement with the CFTC under Commission Regulation 40.2 before it can be listed for trading and clearing. Alternatively, CFTC registered exchanges can seek pre-approval of a new product under Regulation 40.3 prior to listing it for trading and clearing. Bilateral derivatives are not exchange-traded products (ETPs) and are instead governed by documents negotiated directly between the counterparties. Exchanges register with the CFTC as designated contract markets (DCMs) for listed derivatives or swap execution facilities (SEFs) for certain non-retail swap transactions. The CFTC maintains oversight over listed derivatives intermediaries, known as futures commission merchants (FCMs) and introducing brokers (IBs). Separately, the CFTC also regulates clearinghouses for listed derivatives (known as derivatives clearing organizations, or DCOs), swap dealers, commodity pool operators, and commodity trading advisors, among other registrants.

Any derivative product that references a digital asset is listed for trading on a DCM or SEF and executed and cleared in accordance with the CEA or entered into by non-retail market participants on a bilateral basis. DCMs and SEFs are required to comply with core principles under Sections 5 and 5h of the CEA,[178] including CFTC rules related to market integrity, fair access, position limits, pre- and post-trade transparency, and system safeguards.

Once executed on a DCM or (or voluntarily on a SEF), digital asset derivatives are cleared by a registered derivatives clearing organization (DCO), which acts a central counterparty to every buyer and seller. DCOs mitigate counterparty credit risk by guaranteeing the performance of cleared contracts and applying risk management standards under CEA Section 5b.[179] DCOs are required to collect initial and variation margin, maintain default funds, conduct stress testing, and ensure operational resilience.[180]

FCMs, IBs, commodity trading advisors (CTAs), and swap dealers must register with the CFTC and comply with applicable conduct, financial, and recordkeeping requirements under the CEA and CFTC rules. FCMs that handle customer funds for derivative contracts, including digital asset derivatives, must adhere to segregation and safeguarding requirements under Section 4d of the CEA[181] and Parts 1, 22, and 30 of the CFTC's regulations. These protections are designed to ensure that customer property is not misused and that firms can meet their obligations during periods of market stress.

IBs and CTAs are also subject to registration and supervisory requirements under Part 3 of the CFTC's regulations. Additionally, all registered FCMs and IBs must implement and maintain customer identification programs (CIPs) under CFTC Regulation 42.2,[182] which incorporates CIP requirements for FCMs and IBs under the BSA. CIPs requirements include procedures for identity verification, record retention, and screening against certain government watch lists for known or suspected terrorists.[183]

To support regulatory oversight, CFTC registrants and certain market participants are required to report daily transaction and position data to the CFTC under Parts 16, 17, 18, 20, 43, and 45 of the CFTC's regulations. These reporting and recordkeeping requirements enable the CFTC to monitor for systemic risk, large trader activity, and market abuse, and provide the data infrastructure for effective market surveillance and enforcement.

178 7 U.S.C. §§ 7 and 7b-3.
179 7 U.S.C. § 7a-1.
180 *See* 17 C.F.R. §§ 39.13, 39.11, and 39.18 (2024).
181 7 U.S.C. § 6d.

182 17 C.F.R. § 42.2 (2024).
183 31 C.F.R. § 1026.220 (2024).

Even in the case where no derivatives are listed on a particular digital asset commodity, the CFTC maintains anti-fraud and anti-manipulation enforcement authority in the spot markets for such commodities under Section 6(c)(1) of the CEA[184] and CFTC Regulation 180.1.[185] This authority helps ensure that the CFTC can protect market integrity and customer interests in connection with a contract of sale of a commodity in interstate commerce.

The CFTC oversees derivatives on digital asset commodities, primarily bitcoin and ether, on DCMs. For example, the Chicago Mercantile Exchange lists cash-settled bitcoin and etherfutures and options. These derivative contracts are structured to comply with the CEA and CFTC regulations, focusing on transparency, market integrity, and contract enforceability, and are subjectto surveillance,reporting, and position limitrules under Section 5 of the CEA.[186]

Network Tokens

A network token, sometimes called a protocol token, refers to a token that is intrinsically connected to the functioning of a decentralized network or protocol. Importantly, to the extent that a token's network is sufficiently decentralized, its continued value is not dependent on the intervention or control of a single person or group. Some network tokens are used to pay transaction fees (e.g., gas fees) or to stake to secure the network's consensus. Others grant voting rights in a DeFi protocol.[187] Examples of network tokens include bitcoin and ether, each of which derives its value from the blockchain network on which it operates.

Network tokens are issued to allow users to participate in an open decentralized network rather than to provide holders of the token future profit flows from the efforts of a managerial entity. Unlike securities, network tokens do not typically grant equity, debt, or profit-sharing rights. Their value is not derived from a corporate issuer's revenue, but from the utility within the network (for example, demand for block space or voting power). When no single company controls the supply or demand of a token and the token is essential to the ongoing operation of the blockchain network, it begins to resemble a commodity or a type of operational utility token.

Efforts to regulate network tokens should focus on ensuring that tokens, even if initially issued as part of an investment contract in a securities transaction, are not classified as securities once the network becomes fully functional and sufficiently decentralized. Criteria for determining what constitutes "fully functional" and "sufficiently decentralized" should be clear and objective to ensure fairness and provide market participants with certainty.

Tokens for Commercial and Consumer Use

A commercial or consumer use token provides access to some specific good, service, or privilege, and is subject to other federal and state laws applicable to commercial transactions. These tokens are usually non-fungible, meaning they cannot be easily interchanged or substituted with other "like" digital assets. A commercial use token is a digital representation of traditional commercial instruments, such as warehouse receipts, documents of title, bills of lading, event tickets, memberships, and identity credentials. Unlike network tokens, these assets are often not associated with a decentralized network protocol and are usually issued by a centralized entity. Consumer use tokens also include arcade tokens and loyalty tokens that users can redeem for a consumptive purpose, usually within a closed system. Examples of these types of tokens include video game rewards or tokenized loyalty points issued by a company.

184 7 U.S.C. § 9(1).
185 17 C.F.R. § 180.1 (2024).

186 7 U.S.C. § 7.
187 *See* Vitalik Buterin, Ethereum: A Next-Generation Smart Contract and Decentralized Application Platform (2014), https://ethereum.org/content/whitepaper/whitepaper-pdf/Ethereum_Whitepaper_-_Buterin_2014.pdf.

Other variations of consumer use tokens include collectible tokens, such as tokenized artwork, trading cards, and other tokenized versions of traditional collectible items. Often, tokens serve as a record of ownership or otherwise associate ownership rights with a digital identity.

The value of redeemable tokens is derived from the use they provide the holder when redeemed for the relevant good, service, or privilege. Other commercial use tokens may have no intrinsic marketable value (for example, tokens recording identity credentials). Regulation should focus on consumer protections and ensuring that these types of tokens are marketed with appropriate disclosures while allowing companies to experiment with blockchain-based systems. To provide clarity to market participants and ensure innovative uses of blockchain technology for consumer use can continue to grow, regulators may consider some type of guidance, safe harbor framework, or exemptive relief for this asset class.

Enabling the Trading of Digital Assets at the Federal Level

To ensure that American businesses can compete internationally, the SEC and the CFTC should use their existing rulemaking and exemptive authorities to enable the trading of digital assets.

Recommendations

Immediate Actions

The SEC should consider using its rulemaking and exemptive authority under the Securities Act to advance the following initiatives:

- Establish a fit-for-purpose exemption from registration under Section 5 of the Securities Act for securities distributions involving digital assets.
- Establish a time-limited safe harbor or exemption from certain securities law requirements for transactions involving digital assets that may be subject to an investment contract because they are not yet fully functional or associated with a sufficiently decentralized network to allow for progressive functionality or decentralization.
- Establish a safe harbor for certain airdrops from characterization as "sales" under Section 2(a)(3) of the Securities Act or an exemption from the corresponding registration requirements under Section 5 of the Securities Act. Consider also an exemption for distributions of digital assets by decentralized physical infrastructure (DePIN) providers in securities transactions for purposes of rewarding participation in DePIN networks, as well as distributions of certain NFT offerings.

The SEC should consider using its rulemaking and exemptive authority under the Exchange Act to advance the following initiatives:

- Enable non-security digital assets[188] that are tied to an investment contract to be traded on non-SEC registered trading platforms immediately following the primary distribution of the digital asset. • Provide relief for certain DeFi service providers from the broker-dealer (Section 15), exchange (Sections 5 and 6), and clearing agency (Section 17A) registration provisions of the Exchange Act.
- Amend Regulation ATS to (or create a framework similar to Regulation ATS that would) better accommodate trading of non-security digital assets alongside securities under a regulatory framework that is fit-for-purpose for digital asset trading.
- Create a conditional "innovation exemption" under the Exchange Act to allow SEC registrants to engage in

innovative new business models.

188 As used in this report, "non-security digital asset" does not include payment stablecoins. *See supra* note 97 (defining "payment stablecoin").

- Address the definition of "facility" under Section 3(a)(2) of the Exchange Act to consider business models used in digital asset trading.
- Consider amendments to Regulation NMS (or to applicable national market system plans) to better accommodate tokenization of national market system (NMS) securities, or trading of non-security digital assets alongside NMS securities, including requirements applicable to transaction reporting and mechanisms for collecting bids, offers, quotation sizes, and other national market system information. This may include consideration of how amendments could facilitate the use of oracles, aggregators, and other DeFi constructs in the trading of NMS securities and/or non-security digital assets.
- Modernize transfer agent rules to clearly permit the use of blockchain technology by transfer agents. • Provide clarity regarding whether and when self-hosted wallet providers would be acting as broker-dealers subject to SEC registration.

The SEC should consider using its rulemaking and exemptive authority under the Investment Advisers Act, the Investment Company Act, and other applicable laws to advance the following initiatives:

- Provide clarity on the custody of digital assets that are securities for Registered Investment Companies and Registered Investment Advisers by updating the rules under Section 17(f) of the Investment Company Act and Rule 206(4)-2 of the Investment Advisers Act.
- Evaluate whether certain state-chartered trusts should be deemed "qualified custodians," as defined within Advisers Act Rule 206(4)-2(a)(6) or a "bank" under the Investment Company Act.

The CFTC should consider using its rulemaking, interpretative, and exemptive authority under the Commodity Exchange Act (CEA) to advance the following initiatives:

- Provide guidance to designated contract markets (DCMs) regarding the listing of leveraged, margined, or financed spotretail commodity transactions on digital assets pursuantto CEA section 2(c)(2)(D).
- Provide guidance as to how digital assets may be considered commodities under Section 1a(9) ofthe CEA. For example, the agency can consider expanding upon prior guidance on "actual delivery" of virtual assets.[189]
- To the extent that digital asset investment vehicles or their managers may be considered "Commodity Pools" or prompt registration of "Commodity Pool Operators," the CFTC will consider updating rules and guidance as appropriate.
- Collaborate with FinCEN to provide guidance regarding customer identification programs (CIPs) utilizing new technologies for eligible intermediaries and other market participants who carry customer accounts holding digital assets on behalf of customers.[190] This collaboration can explore intermediaries' and other market participants' reliance on other financial institutions' identification and verification functions. • Enable firms to provide bundled trading and custody services.
- Provide clarity on the applicability of various CFTC registration requirements to DeFi activities, smart contract protocols, or decentralized autonomous organizations (DAOs) consistent with technology-neutral principles. • Provide guidance to FCMs in calculating and administering segregation obligations when digital assets are held on behalf of customers, including separate account treatment under Regulation 1.44. • Provide clarity on haircuts on digital assets held by registered intermediaries (including FCMs, swap dealers, and DCOs) for purposes of calculating and reporting margin, financial resources/capital,

189 *See* 85 Fed. Reg. 37734, *supra* note 96. Furthermore, the CFTC's Global Markets Advisory Committee considered a variety of digital assets issues, including proposing a taxonomy for digital assets. *See* CFTC Global Markets Advisory Committee Digital Asset Markets Subcommittee, Digital Assets Classification Approach and Taxonomy (Mar. 6, 2024), https://www.cftc.gov/media/10321/CFTC_GMAC_DAM_Classification_Approach_and_Taxonomy_for_Digital_Assets_030624/download.

190 *See* 31 C.F.R. § 1026.220(a)(6) (2024); *Anti-Money Laundering: Customer Identification Programs*, CFTC, https://www.cftc.gov/IndustryOversight/AntiMoneyLaundering/dsio_aml_cia.html (last visited July 13, 2025).

segregation, and settlement obligations, including working with the SEC around the non-marketable securities haircut framework and its applicability to non-security digital assets.

- Review the application of eligible depository rules to accounts holding digital assets as collateral under CFTC Regulation 1.49.
- Provide guidance for DCO acceptance of digital asset collateral (including payment stablecoins)[191] including DCO financial resource requirements, valuation of assets and haircuts for margin purposes, settlement finality, treatment of digital asset custodians and self-custody, systems safeguards requirements, end-of day reporting for assets that trade 24/7, and legal risk considerations in such areas as netting and interests in collateral under CFTC Regulations 39.11, 39.13, 39.14, 39.15, 39.18, 39.19, and 39.27.
- Provide guidance on the adoption of tokenized non-cash collateral as regulatory margin to implement the CFTC's GMAC DAMS recommendation.
- Provide guidance on the classification of swaps on digital assets to address application of margin, reporting, and other requirements under CFTC Regulations 1.3, 23.154, 43.2, and 45.1.
- Consider allowing the use of blockchain technology to satisfy recordkeeping obligations under CFTC Regulation 1.31.

The SEC and the CFTC should coordinate to ensure efficient rulemaking processes. The SEC and CFTC should coordinate on seeking comments from the public on suggestions for rulemaking.

If the SEC and CFTC establish a regulatory sandbox or safe harbor, it should have clear criteria to determine which types of digital assets and market participants are eligible for the sandbox or safe harbor. Moreover, there should be a clear pathway for entities to graduate from the sandbox or safe harbor.

In coordination with the SEC, the CFTC should consider using its authority within CEA section 1a(18) to establish a category of eligible contract participants (ECPs) with the ability to engage in certain types of derivatives, including perpetual contracts, through additional regulated intermediaries (e.g., persons that are counterparties to a specified transaction conducted on or pursuant to the rules of an alternative trading system).

Longer-Term Considerations

The SEC and CFTC should explore offering flexibility to allow registrants to offer multiple services within a single user interface.

- The Working Group encourages regulatory exploration of more vertically integrated business models in the digital asset space. These business models should include appropriate structural safeguards, governance mechanisms, and disclosures to mitigate conflicts of interest.
- While addressing conflicts and ensuring existing registrants are not disadvantaged, regulators may consider adopting regulatory regimes that allow registrants to integrate multiple financial services in one business model, which could further reduce frictions and enhance user experience.
  - Combining exchange services with custody of trading assets allows for real-time settlement. The custodian holds the assets, and the exchange matches orders to buy and sell those assets.

Additionally, the digital assets custodied by an exchange should be cryptographically verifiable.

◆ Combining exchange and broker services allows for economies of scale and reduces operational complexity by permitting straight-through processing of customer orders with the same technology stack. ◆ Exchanges and intermediaries must segregate customer property away from proprietary funds, subject to reasonable exceptions.

191 *See supra* note 97 (defining "payment stablecoin").

The CFTC should consider how existing rules could be amended to enable the use of blockchain-based derivatives.

- Such considerations should include evaluating the benefits of blockchain-based derivative transactions or systems with respect to the regulatory requirements of central clearing, and frameworks around reporting obligations, margin levels, and contract listings in a non-intermediated environment.

Absent congressional action, the SEC and CFTC should use their existing authorities to provide fulsome regulatory clarity that best keeps blockchain-based innovation within the United States.

- As discussed below, the Working Group strongly recommends that Congress expeditiously advance market structure legislation to the President's desk.
- However, as market structure deliberations continue in Congress, the Working Group similarly recognizes that the market regulators can work to provide appropriate accommodation for digital asset trading and innovation in their rules to ensure responsible innovation occurs in the United States.

Creating a Lasting Framework for Digital Asset Market Structure

Due to the underlying distributed ledger technology, digital asset markets function differently from markets for stocks, bonds, commodities, and derivatives. Traditional financial markets require a series of third party intermediaries between a buyer and a seller to execute and settle a trade. In digital asset markets, programmable smart contracts allow buyers and sellers of certain digital assets on decentralized exchanges to be matched and ownership to change hands without a custodial third-party. Other platforms offering trading of digital assets are structured in a more centralized way, but differences remain that need to be addressed in crafting a market structure framework.

The House of Representatives' Digital Asset Market Clarity Act of 2025 (CLARITY)[192] proposes a division of digital asset market jurisdiction between the SEC and CFTC. It protects the right of Americans to self-custody their digital assets. By requiring the SEC and CFTC to jointly promulgate rules for portfolio margining, it facilitates a system where investors, both retail and institutional, can efficiently trade digital assets without artificial costs imposed by regulatory barriers.

CLARITY also importantly recognizes decentralized governance systems, which are an innovation in how individuals collectively reach agreement on development and administration of blockchain systems. Much as joint stock corporations provided an avenue for shareholders to engage in common undertakings, decentralized governance systems are a further evolution in decision-making. CLARITY recognizes the promise of decentralized finance and the ability of software to allow individuals to freely transact with one another.

Lastly, CLARITY provides legal certainty in highlighting the treatment of digital assets on banking institutions' balance sheets, providing federal pre-emption for jurisdiction over digital asset intermediaries, and explaining the criteria by which institutions can be considered Qualified Custodians of digital assets.

Altogether, CLARITY represents an excellent foundation for digital asset market structure in the United States. However, the Working Group encourages Congress to consider a handful of additional factors when finalizing this legislation to ensure American markets for digital assets help enshrine the United States as the crypto capital of the world.

192 H.R. 3633, 119th Cong. (2025).

Recommendations

Congress should consider the following when finalizing provisions of market structure legislation to ensure the most cost-efficient and pro-innovation regulatory structure for digital assets.

Jurisdiction of Market Regulators

The CFTC should have clear authority to regulate spot markets in non-security digital assets. SEC and CFTC registrants should be permitted to engage in multiple business lines under the most efficient licensing structure possible, ensuring a clear and simple regulatory framework for digital asset market activities.

- Regulation should be crafted to avoid regulatory arbitrage between the SEC and CFTC digital asset regulatory regimes, understanding that the regulation of digital asset securities is necessarily different than that applied to non-security digital assets. Interagency coordination could guide these efforts.
- Registrant platforms should have the flexibility to offer a broad range of digital asset and other regulated products within a single user interface, subject to clearly defined regulatory oversight of the registrant. • SEC registrants should be able to offer the trading of digital asset securities and be able to engage in non security digital asset transactions pursuant to the licensing structure defined by Congress. • CFTC registrants should be able to offer the trading of digital commodity derivatives, retail digital commodity transactions, and other CFTC-jurisdictional products alongside non-security digital assets, as specified by Congress.
- To the extent Congress permits activity in non-security digital assets outside CFTC registrants, Congress should direct the market regulator leading the rulemaking process to set rules for market conduct and activities for non-security digital assets in consultation with the SEC or CFTC, as appropriate.
- Rules for digital assets should include portfolio margining standards, as suggested by CLARITY.[193] • The SEC and CFTC should adopt rules ensuring customer asset segregation for digital assets.[194] • Trading venues for non-security digital assets should be required to report market data, subject to reporting obligations established by the CFTC. If a trading venue is engaged solely in the provisioning of non-security digital assets, there should only be reporting obligations to the CFTC.
    - ◆ Prior to the enactment of any reporting obligations, the CFTC should consult with the SEC on the data to be reported and the format in which it is reported to minimize industry burden.

Congress should provide that federal law preempts state law with respect to securities and commodities laws applicable to SEC- and CFTC-registered intermediaries, including in the areas of state virtual currency business, “blue sky,” and commodity broker laws.

193 *See* H.R. 3633, 119th Cong. § 105(e) (2025).
194 Note that the CFTC-registered futures commission merchants (FCMs) already have segregation obligations under current law. *See* CFTC, *Futures Commissions Merchants (FCMs): Segregation of Customer Funds*, https://www.cftc.gov/IndustryOversight/Intermediaries/FCMs/fcmsegregationfunds (last visited July 13, 2025). In 2020, the Division of Swap Dealer and Intermediary Oversight of the CFTC issued a staff letter advisory as to how FCM segregation obligations apply to virtual currency. CFTC Letter No. 20-34, Accepting Virtual Currencies from Customers into Segregation (Oct. 21, 2020), https://www.cftc.gov/csl/20-34/download.

Guidelines for Market Intermediaries

Digital asset trading platforms, brokers, dealers, custodians and other registrants should be subject to a tailored registration regime that is fit-for-purpose under the SEC or CFTC, as appropriate and based upon the intermediary's activities.

- Consistent with the existing financial markets regulatory framework, the regime should include principles based requirements that are no more onerous than those safeguards applied to existing registrants.

Intermediaries should be allowed to lend against, net, and hedge securities against non-securities, as risk characteristics permit.

- Coordinated regulatory treatment can ensure appropriate market oversight, while recognizing economic equivalence across different asset types.
- The SEC and CFTC should have appropriate flexibility in setting applicable rules for their registrants.

Issuers of digital asset securities, and of securities involving digital assets, should be subject to disclosure requirements that are appropriately tailored to address the novel characteristics of digital assets and blockchain technology. Digital asset trading platforms, brokers, dealers, and other CFTC registered intermediaries that make available non-security digital assets should be required to disclose any such information that the CFTC determines to be appropriate for non-security digital assets.

- Further, these parties should not be subject to ongoing disclosure requirements other than those required by Congress in future legislation or by the relevant market regulator. Furthermore, any such ongoing disclosures should be fit-for-purpose and guided by publicly available information, such as open-source code, whenever possible.
- Digital asset trading platforms, and other intermediaries as appropriate, should publish the criteria that govern the listing of digital assets that are traded.
  - ◆ In addition, digital asset trading platforms, and other intermediaries as appropriate, should consider prominently disclosing features that may be unique to digital assets, such as token economics (i.e., allocation percentages and rationales) and source code, if applicable.

For institutional over-the-counter block trades of digital assets that occur offchain through regulated intermediaries, there should be similar reporting and disclosure requirements to those that apply to similar activities in traditional markets.

- These reporting and disclosure requirements need not be instantaneous, but it is critical to ensure there are not loopholes or "blind spots" associated with digital asset trading activity that occurs offchain.

Digital asset trading platforms, brokers, dealers, and other SEC and CFTC registrants should disclose the capacity in which they are acting on behalf of the customer, client, or counterparty (i.e., dealer, broker, counterparty, routing to an order book, etc.).

- Digital asset firms may serve in a variety of capacities when offering digital asset trading. Congress should consider disclosure requirements or standards depending on the nature of the relationship between the firm and the market participant (e.g., retail, institutional, customer, client, counterparty, etc.).

Trading platforms should be permitted to custody customer digital assets with appropriate controls.

- Safeguards may include requirements for asset segregation, disclosures, principles-based cybersecurity standards, bankruptcy remoteness, separation of legal entities, separation from margin and rehypothecation entity, capital requirements, liquidity and redemption requirements, and regulatory supervision.

- Trading platforms should also enable users engaging in self-custody to transact, and should be prohibited from discriminating against third-party custodians who offer products that compete with those provided by the trading platform or an affiliate.

Market intermediaries should be subject to principles-based rules regarding the margin and leverage they can extend to retail participants, based on the functions of margin and leverage in their respective activities. Congress should clearly define the rules and responsibilities between the SEC and CFTC regarding margin and leverage, but allow the regulators appropriate flexibility in setting such rules.

- Financing rates offered to retail customers should be publicly disclosed by the party offering leverage.

Congress should consider extending Exchange Act Section 31 fee structures to all SEC-registered products offered on SEC-regulated platforms.

- Intermediaries offering digital asset services should pay fees equivalent to those that traditional finance intermediaries pay in the equity markets.

SEC and CFTC registrants should be required to adopt best practices for cybersecurity standards.

- These standards may be adopted as part of a principles-based regulatory framework or proposed as industry best practices.

Regulatory Treatment of DeFi

By embracing and supporting the option of DeFi for investors, policymakers can help position the United States as a leader in the global crypto economy. Encouraging the development of regulatory frameworks that balance innovation with security will pave the way for a robust financial future. The integration of DeFi into mainstream finance has the potential to unlock new economic opportunities and drive significant advancements across various industries and sectors.

There are ongoing discussions regarding whether non-controlling blockchain developers, DeFi service providers, and DeFi apps orfront ends can or should be required to comply with institutional obligations underthe Bank Secrecy Act (BSA), either as money services businesses (MSBs), broker-dealers, FCMs, or some other category of "financial institution" underthe BSA.[195] Such considerations are discussed further in the *Further Improvements to the AML/CFT Regime* section of Chapter VI, covering topics related to countering illicit finance.

As contemplated in provisions of CLARITY,[196] Congress should consider the following factors when determining the regulatory treatment of DeFi:

- The extent to which a given software application exercises "control" over user assets.
  - ◆ Without the ability to exercise control over user assets or funds, a software application may not transmit money or exchange currency, and therefore might not be subject to the BSA as an MSB. Importantly, without control, software applications generally lack the ability to misappropriate user assets.
- The extent to which a given software application, once built or deployed, is technologically capable of being modified.

195 *See* 31 U.S.C. § 5312(a)(2) and 5312(c).

196 *See* Press Release, Representative Tom Emmer, Emmer's Securities Clarity Act and Blockchain Regulatory Certainty Act Pass House Financial Services Committee Markup (June 11, 2025), https://emmer.house.gov/media-center/press-releases/emmer-s-securities-clarity-act-and-blockchain-regulatory-certainty act-pass-house-financial-services-committee-markup (noting that the "elements of the Blockchain Regulatory Certainty Act that are include in the CLARITY Act codify that digital asset developers and service providers that do not custody consumer funds are not money transmitters.").

  - ◆ Software applications in DeFi use smart contracts. In many cases, smart contracts cannot be modified or withdrawn once deployed. Implementing changes in those cases requires the creation of entirely new smart contracts.
  - ◆ The operations of a software application, including the smart contracts or the economics of the service more broadly, may be administered by a single actor or a group of actors working together. ◆ As such, Congress should consider the degree to which a single actor, or group of actors working together, has the unilateral ability to upgrade a software application's smart contracts or change its economics in a manner not previously disclosed in the software or protocol rules.
- The extent to which a software application is controlled by, or operates with, a centralized structure or management.
  - ◆ If a product or service is operated, managed, or otherwise controlled by a business and facilitates access to a DeFi system engaged in otherwise regulated activity, that product or service should be subject to regulation accounting for underlying regulated activity and pursuant to the principles of fair competition, customer protection, conflicts of interest, integrity of code, cybersecurity standards, and other principles as appropriate.
- The extent to which a given software application is technologically or logistically capable of complying with current regulatory obligations.
  - ◆ Many DeFi protocols and non-controlling blockchains do not have the functional ability to register as MSBs or otherwise comply with MSB obligations under the BSA, while businesses (as described above) could register. Nevertheless, Congress could consider how obligations can be fit-for-purpose to the technology and embrace the unique characteristics of DeFi, rather than placing the current financial regulatory regime on top of DeFi services.
  - ◆ Care should be taken to ensure that actors are not permitted to structure products to subvert legal responsibilities.

Accounting Recommendations

Financial Accounting Standards Board (FASB)[197] processes include outreach to a broad set of stakeholders including investors, preparers, accounting firms, academics, and regulators.[198] The FASB issued accounting guidance in December 2023 addressing the subsequent measurement of certain digital asset holdings at

fair value.[199] It has also specifically requested stakeholder input on any additional accounting guidance needed to address digital asset matters under U.S. Generally Accepted Accounting Principles (GAAP).[200]

The Working Group observed that many questions on the accounting for digital asset transactions relate to the following key concepts that FASB should consider for further consultation through public engagement:

- Recognition and derecognition: Whether an entity should recognize or derecognize digital asset tokens when entering into certain transactions. For example, should a lender of digital assets derecognize such assets, and should there be symmetry in accounting between a lender and borrower? Similar questions may arise related to wrapping tokens or transacting with decentralized lending or exchange protocols.

197 The SEC has recognized the FASB's accounting standards as authoritative since 1973. *See* SEC, Policy Statement: Reaffirming the Status of the FASB as a Designated Private-Sector Standard Setter (Apr. 25, 2003) https://www.sec.gov/rules-regulations/policy-statements/33-8221. 198 *See* Financial Accounting Standards Board (FASB), Rules of Procedure: Amended and Restated Through February 12, 2025 (2025), https://www.fasb.org/page/ShowPdf?path=Rules%20of%20Procedure-Feb%202025.pdf&title=Rules%20of%20Procedure-February%202025.

199 FASB, Accounting Standards Update No. 2023-08, Accounting for and Disclosure of Crypto Assets (Dec. 2023), https://www.fasb.org/page/PageContent?pageId=/projects/recentlycompleted/accounting-for-and-disclosure-of-crypto-assets.html.

200 FASB, Invitation to Comment: Agenda Consultation (Jan. 3, 2025), https://fasb.org/page/ShowPdf?path=ITC%E2%80%94Agenda%20Consultation.pdf&title=Invitation%20to%20Comment%E2%80%94Agenda%20Consultation.

- Issuer accounting. How an entity should account for digital asset tokens it creates and issues. The accounting by the token issuer will depend on the issuer's facts and circumstances, and the enforceable rights and obligations of the parties involved. To the extent a token conveys rights or obligations that align with traditional assets or instruments (e.g., ownership of tangible commodities, debt, or equity), then established accounting guidance already exists. Additionally, FASB should consider whether to treat payment stablecoins as cash equivalents under GAAP. Further clarification is required in cases where tokens provide utility or access without clearly enforceable rights – particularly when tied to the future development of a platform. There is no explicit guidance to address the accounting for those types of token issuances.

Additionally,the principles-based nature ofthe Public Company Accounting Oversight Board's (PCAOB's) audit standards and guidance published by the PCAOB, as well as non-authoritative guidance from the American Institute of Certified Public Accountants (AICPA), have allowed auditors of public companies and broker dealers to adapttraditional procedures to address digital assettokens. As the technology and its use continues to develop,there may be value in additional or new standards to promote consistency in application and execution and help align regulatory and stakeholder expectations (avoiding expectation gaps).

International Regulatory Standards and Landscape

TheWorking Group advises the United States to reassert global leadership on digital assets. Reassertion of such leadership depends on establishing a clear and robust policy framework for digital asset activity. Large financial centers like the European Union (EU), Japan, Singapore, and the United Kingdom (UK) are finalizing and implementing their own digital assetframeworks, offering a foundation upon which they seek to attract firms and grow their markets. The United States has a window of opportunity to shape the way these frameworks intersect and interact, fostering a level playing-field on which American firms and markets can compete with the rest of the world. As such, the Working Group advises the United States to engage and lead internationally to achieve these objectives.

In parallel, some digital asset firms have chosen to operate globally out of smaller jurisdictions, some of which have become significant centers for digital asset activity, but which may lack adequate regulation, effective supervision, or enforcement capacity to oversee that activity, including illicit finance controls (see Chapter VI), which discusses the regulatory framework around illicit finance as pertains to digital assets). A clear and robust U.S. framework will serve as a standard and indicator of credibility for firms that onshore their activities in the United States. Paired with active U.S. leadership in international engagement, an American regulatory framework will also serve to discourage firms from operating in jurisdictions that compete with inadequate regulation, supervision, and enforcement.

International Standards

U.S. regulators, including the Department of Treasury and its Office of International Financial Markets, have been active in international discussions to shape emerging regulatory standards for digital assets, recognizing emerging best practices as authorities develop their respective domestic regulatory frameworks. In July 2023, the Financial Stability Board (FSB) published its global regulatory framework for digital asset activities. The framework includes high-level recommendations for the regulation, supervision, and oversight of digital asset activities and markets and of widely used stablecoins. These recommendations promote the creation of risk-based regulatory regimes, in which digital asset issuers and service providers have adequate governance, risk management, and disclosure obligations,

including for potential conflicts of interest.[201] The Working Group suggests that the United States advance policies at the FSB aligned with recommendations for digital asset regulatory frameworks outlined in this report.

In addition, the Financial Action Task Force (FATF), the international standard setting body for AML/countering the financing of terrorism (CFT), clarified under the 2018 U.S. presidency that its standards apply to virtual assets and virtual asset service providers (VASPs).[202] The FATF recommended that jurisdictions must assess risk associated with virtual assets and require that VASPs in their jurisdiction are regulated and supervised for implementation of AML/CFT obligations. The Working Group would be supportive of adopting several FATF standards for virtual assets, consistent with recommendations in this report, and advises the United States to remain a leader on FATF efforts on this topic.

Other financial sector standard-setting bodies have also addressed market conduct and capital standards for digital assets activity in financial markets and banking. The International Organization of Securities Commissions in 2023 published high-level guidance for, among other policies, addressing market abuse, digital asset custody arrangements, and trading disclosures.[203] In 2022, the Basel Committee on Banking Supervision (BCBS) published capital standards for banks' exposure to cryptoassets and stablecoins.[204] This framework, which was later amended in 2024[205] and is discussed in further detail later in this report, assigns risk weights reflecting the BCBS's assessment of different types of cryptoassets and the ledgers on which they trade; it assigns the highest risk weight to cryptoassets traded on permissionless ledgers. Where standards are misaligned, the Working Group advises that the United States assert leadership and advocate that relevant bodies develop guidance in line with the goals of the Working Group to establish the United States as a global leader on digital assets regulation.

Evolving Regulatory Landscape

Large financial-center jurisdictions have developed their own separate regimes for the regulation of digital assets, with some common features.[206] Common elements of current and proposed stablecoin regimes in the EU, Hong Kong, Singapore, Japan, and the UK include: a licensing regime; reserve and other prudential requirements; requirements to segregate customer assets from those of the digital asset service provider itself; provisions for client redemption rights; mandatory disclosures and periodic audits; varying prohibitions on algorithmic stablecoins; and AML/CFT obligations. Similarly, emerging digital asset market structure regimes around the world restrict advertising for consumer protection and prevent market abuse, broadly equivalent to traditional financial market rules, although the details of these restrictions vary.

However, many regulatory regimes are not comprehensive and may require expansion or updating. The EU's Markets in Crypto-Assets (MiCA) Regulation exemplifies a comprehensive global digital assets

201 *See* Financial Stability Board, High-Level Recommendations for the Regulation, Supervision and Oversight of Crypto-Asset Activities and Markets: Final report (July 17, 2023), https://www.fsb.org/2023/07/high-level-recommendations-for-the-regulation-supervision-and-oversight-of-crypto-asset-activities-and markets-final-report.

202 *See generally* Financial Action Task Force, Updated Guidance for a Risk-Based Approach: Virtual Assets and Virtual Asset Service Providers (Oct. 2021), https://www.fatf-gafi.org/content/dam/fatf-gafi/guidance/Updated-Guidance-VA-VASP.pdf.coredownload.inline.pdf.

203 *See generally* International Organization of Securities Commission, Policy Recommendations for Crypto and Digital Asset Markets: Final Report (Nov. 16, 2023), https://www.iosco.org/library/pubdocs/pdf/IOSCOPD747.pdf.

204 Basel Committee on Bank Supervision (BCBS), Prudential Treatment of Cryptoasset Exposures (Dec. 2022), https://www.bis.org/bcbs/publ/d545.pdf., 205 BCBS, Cryptoasset Standard Amendments (July 2024), https://www.bis.org/bcbs/publ/d579.pdf.

206 For an overview of global approaches to digital assets policy, *see Cryptocurrency Regulation Tracker*, The Atlantic Council, https://www.atlanticcouncil.org/programs/geoeconomics-center/cryptoregulationtracker (last visited July 13, 2025).

regime currently in force.[207] European authorities adopted MiCA in late 2024, but some European policy makers have already called for a "MiCA 2" to address gaps in the new rules. These gaps include, at least, limited jurisdiction over digital asset service providers operating from outside Europe and omission of DeFi, NFTs, and digital asset lending.

Similarly, Japan was an early leader in the regulation of digital asset activities and was, in 2014, among the first countries to legally define and classify digital assets. However, Japan has subsequently amended its framework to accommodate the maturing global digital asset market. In April 2025, Japan's Financial Services Agency announced a new approach to digital assets, including reclassifying these assets as financial products and has signaled its intention to recalibrate its stablecoin reserve requirements to retain global competitiveness.

The evolution of digital asset frameworks in other large financial centers across the globe creates an opportunity for the United States to shape global regulatory standards and norms in ways that align with U.S. interests. It also creates an opportunity for the United States to support a less fragmented
digital asset ecosystem, with fewer unwarranted regulatory frictions, which can better support the allocation of capital to its most efficient use.

Regulatory Fragmentation

Regulatory fragmentation among jurisdictions with different—or even conflicting—regimes could impact market flows of digital assets. For stablecoins, a lack of broad, coherent, and robust oversight can undermine stablecoins'reliability as a paymentinstrument, limiting their circulation,their stability, ortheir ability to circulate without discount. Regulatory fragmentation can also lead to

marketfragmentation, and to reduced ortrapped liquidity within specific stablecoin arrangements;this, in turn, can limit market depth in ways that can affectthe broader health of digital asset markets. More fundamentally, fragmentation may impose inefficient compliance and operational costs on U.S. stablecoin issuers and other registrants operating internationally, making them less competitive and the international playing field less even. This is true also for digital asset markets, in which existing frameworks diverge with respectto legal classifications,taxation, margin trading, staking, and other areas.

A robust U.S. policy framework for digital assets can help minimize these risks and promote the growth of the digital asset industry globally. U.S. engagement on these issues must prioritize U.S. interests— including an innovative, fair, open, and efficient digital asset ecosystem.

207 *See* Financial Stability Board, *FSB Notes Significant Progress in Monitoring, Regulating and Supervising Crypto-Asset Activities in France* (Dec. 11, 2024), https://www.fsb.org/2024/12/fsb-notes-significant-progress-in-monitoring-regulating-and-supervising-crypto-asset-activities-in-france.

IV. Banking and Digital Assets

CHAPTER IV

Banking and Digital Assets

Banking and Digital Assets

> Commerce on the Internet has come to rely almost exclusively on financial institutions serving as trusted third parties to process electronic payments. While the system works well enough for most transactions, it still suffers from the inherent weaknesses of the trust based model.
>
> Introduction from *Bitcoin: A Peer-to-Peer Electronic Cash System*
> Satoshi Nakamoto, October 2008[208]

The genesis block of Bitcoin, the first block ever mined, famously contains a headline from the day it was created: "The Times 03/Jan/2009 Chancellor on brink of second bailout for banks."[209] Though Satoshi was cautious of banks, the technology and industry that evolved from his work would come to interact with the banking system in unexpected ways. Some banks, recognizing the promise of the space, began providing core banking services to growing crypto enterprises. Others, building on their banking-as-a-service offerings to fintech companies, supported new clients engaged in digital assets. Additionally, some "crypto banks"[210]— chartered financial institutions offering the ability to buy, sell, and custody digital assets alongside traditional banking services, such as access to traditional fiat payment rails—emerged and blurred the line between the TradFi and crypto-native worlds.[211] Outside the traditional banking sector, the growth in retail access to digital assets has created opportunities for unbanked Americans to access the financial system. A survey from May 2025 indicated that 10% of cryptocurrency owners stated they owned cryptocurrency

before opening a checking account, savings account, or an account with certain common payments apps.[212]

Although many in the banking industry supported the growth and development of the crypto ecosystem, regulatory leadership set up roadblocks. The Biden Administration's Operation Choke Point 2.0 resulted in the widescale debanking of digital asset firms and their founders. As Acting Federal Deposit Insurance Corporation (FDIC) Chairman Travis Hill noted in February 2025 when publishing internal documents related to the FDIC's supervision of banks that engaged in, or sought to engage in, crypto-related activities:

> [T]he FDIC's approach "has contributed to a general perception that the agency was closed for business if institutions are interested in anything related to blockchain or distributed ledger technology." . . . The documents that we are releasing today show that requests from these banks were almost universally met with resistance, ranging from repeated requests for further information . . . to directives from supervisors to pause, suspend, or refrain from expanding all crypto- or blockchain-related activity. Both individually and collectively, these and other actions sent the message to banks that it would be extraordinarily difficult—if not impossible—to move forward. As a result, the vast majority of banks simply stopped trying.[213]

208 Nakamoto, *supra* note 18.

209 *See* mempool.space (Jan. 3, 2009), https://mempool.space/block/0000000000019d6689c085ae165831e934ff763ae46a2a6c172b3f1b60a8ce26f. *See also* Jon Southurst, *Bitcoin Genesis Block Constructed 11 Years Ago Today*, CoinGeek (Jan. 3, 2020), https://coingeek.com/bitcoin-genesis-block-constructed-11- years-ago-today.

210 Note that such "crypto banks," which either hold state charters or an OCC national trust bank charter, do not necessarily offer the full range of traditional banking services, absent additional approvals.

211 Coin World, *Crypto Firms Expand into Traditional Finance, Blurring Lines with New Offerings,* AInvest (Apr. 25, 2025, 2:07 PM ET), https://www.ainvest.com/news/crypto-firms-expand-traditional-finance-blurring-lines-offerings-2504.

212 Justin Slaughter & Dominique Little, *Paradigm Policy Market Mapping Exercise Spring 2025*, Paradigm (July 1, 2025), https://www.paradigm.xyz/2025/07/paradigm-policy-market-mapping-exercise-spring-2025.

213 *See* FDIC, *FDIC Releases Documents Related to Supervision of Crypto-Related Activities*, (Feb. 5, 2025), https://www.fdic.gov/news/press-releases/2025/fdic-releases-documents-related-supervision-crypto-related-activities; *see also Hist. Assocs. Inc. v. FDIC*, No. 1:24-cv-1857-ACR (D.D.C.).

Under the Trump Administration, Operation Choke Point 2.0 is dead—not just in spirit, but in substance. The Securities and Exchange Commission (SEC) staff rescinded Staff Accounting Bulletin (SAB) No. 121, an accounting guidance that effectively prohibited publicly traded banks from offering custody services for digital assets.[214] The FDIC rescinded a prior-notification requirement for supervised institutions in March 2025, and affirmed that banks under their purview "may engage in permissible activities, including activities involving new and emerging technologies such as crypto-assets and digital-assets, provided that they adequately manage the associated risks."[215] That month, the Office of the Comptroller of the Currency (OCC) published Interpretive Letter No. 1183, confirming that national banks and federal savings associations may engage in digital asset custody, stablecoin-related activities, and use blockchains to facilitate payments without seeking prior approval.[216] The OCC also announced that it would no longer examine banks for "reputation risk," and the Board of Governors of the Federal Reserve System (FRB) announced the same in June.[217] Then, in April, the FRB rescinded two supervisory letters related to banks' "crypto-asset and dollar token activities," with the express purpose of ensuring the FRB's "expectations remain aligned with evolving risks and further support innovation in the banking system."[218]

By April 2025, the OCC, FDIC, and FRB had all withdrawn from joint statements issued in January and February 2023 cautioning banking organizations against engaging in digital asset activity.[219] And in July 2025, the OCC, FDIC, and FRB issued a new joint statement reaffirming the legal permissibility for banks to custody digital assets.[220] In contrast to the Trump Administration's leadership, the Biden Administration endorsed that now

214 SAB No. 121 mandated that certain entities safeguarding digital assets record both a liability and a corresponding asset on their balance sheets at the fair value of the assets held, even if such assets were never lent by the entities. Staff Accounting Bulletin No. 121, 87 Fed. Reg. 21015 (Apr. 11, 2022) (formerly codified at 17 C.F.R. pt. 211 (2024)). SAB No. 121 was rescinded by a new staff accounting bulletin, SAB No. 122. Staff Accounting Bulletin No. 122, 90 Fed. Reg. 8492 (Jan. 30, 2025) (codified at 17 C.F.R. pt. 211 (2024)). SEC Staff Accounting Bulletins are not rules or interpretations of the SEC, nor are they published as bearing the SEC's official approval. They represent interpretations and practices followed by the SEC Division of Corporation Finance and the SEC Office of the Chief Accountant in administering the disclosure requirements of federal securities laws. Note that the Guiding and Establishing National Innovation for U.S. Stablecoins Act (GENIUS), which was signed into law by President Trump on July 18, 2025 prohibits the SEC, FDIC, OCC, FRB, and NCUA from adopting rules for public and private depository institutions similar to SAB No. 121. S. 1582, 119th Cong. (2025) § 16(c) (enacted).

215 Press Release, FDIC, FDIC Clarifies Process for Banks to Engage in Crypto-Related Activities (Mar. 28, 2025), https://www.fdic.gov/news/financial-institution letters/2025/fdic-clarifies-process-banks-engage-crypto-related.

216 OCC, Interpretive Letter No. 1183, OCC Letter Addressing Certain Crypto-Asset Activities (Mar. 7, 2025), https://www.occ.gov/topics/charters-and-licensing/ interpretations-and-actions/2025/int1183.pdf. The OCC subsequently issued Interpretive Letter No. 1184, which provided further clarity on permissible custody activities. *See* OCC, Interpretive Letter No. 1184, Clarification of Bank Authority Regarding Crypto-Asset Custody Services (May 7, 2025), https:// www.occ.gov/topics/charters-and-licensing/interpretations-and-actions/2025/int1184.pdf.

217 *OCC Ceases Examinations for Reputation Risk*, OCC (Mar. 20, 2025), https://www.occ.gov/news-issuances/news-releases/2025/nr-occ-2025-21.html; *Federal Reserve Board Announces That Reputational Risk Will No Longer Be a Component of Examination Programs in Its Supervision of Banks*, FRB (June 23, 2025), https://www.federalreserve.gov/newsevents/pressreleases/bcreg20250623a.htm. The FDIC is also "working on a rulemaking related to reputation risk that would prohibit FDIC supervisors from (1) criticizing or taking adverse action against institutions on the basis of reputational risk and (2) requiring, instructing, or encouraging institutions to close, modify, or refrain from offering accounts on the basis of political, social, cultural, or religious views." Acting Chairman Travis Hill, FDIC, Speech at American Bankers Association Washington Summit: View from the FDIC: Update on Key Policy Issues (Apr. 8, 2025), https://www.fdic.gov/news/speeches/2025/view-fdic-update-key-policy-issues.

218 Press Release, FRB, Federal Reserve Board Announces the Withdrawal of Guidance for Banks Related to Their Crypto-Asset and Dollar Token Activities and Related Changes to Its Expectations for These Activities (Apr. 24, 2025), https://www.federalreserve.gov/newsevents/pressreleases/bcreg20250424a.htm.

219 *See id.; see also* FRB, FDIC & OCC, Joint Statement on Crypto-Asset Risks to Banking Organizations (Jan. 3, 2023), https://www.federalreserve.gov/newsevents/pressreleases/files/bcreg20250424a1.pdf; FRB, FDIC & OCC, Joint Statement on Liquidity Risks to Banking Organizations Resulting from Crypto-Asset Market Vulnerabilities (Feb. 23, 2023), https://www.federalreserve.gov/newsevents/pressreleases/files/bcreg20250424a2.pdf. Silvergate Capital Corporation, the parent company of one of the banks that failed in March 2023, disclosed risk in a public filing on March 1, less than two weeks before it announced plans to wind down and self-liquidate, that "the safety and soundness concerns expressed by the federal banking agencies regarding banking institutions with business models that are concentrated in digital asset related activities" could cause its financial performance to differ materially from its projections. Silvergate Capital Corporation, Form 12b-25 (Mar. 1, 2023), https://www.sec.gov/Archives/edgar/data/1312109/000110465923027353/tm238251d1_nt10k.htm. Similarly, former Congressman Barney Frank, one of the Board members of Signature Bank, which was forcibly closed by the New York State Department of Financial Services (NYDFS) in March 2023, speculated that NYDFS was "using us as a poster child to say 'stay away from crypto.'" Jen Wieczner, *Barney Frank Talks More About the Surprise Shuttering of Signature Bank*, N.Y. Magazine (Mar. 15, 2023), https://nymag.com/intelligencer/2023/03/barney-frank-says-more-shuttering-signature-bank.html.

220 FRB, FDIC &OCC, Crypto-Asset Safekeeping byBankingOrganizations (July 14, 2025), https://www.occ.gov/news-issuances/news-releases/2025/nr-ia-2025-68a.pdf.

rescinded January 2023 guidance and encouraged regulators to continue efforts designed to "limit financial institutions' exposure to the risks of digital assets."[221]

Regulatory efforts to deny banking services to the digital asset industry have ceased under the Trump Administration. With growth now in focus, the Working Group supports banks' participation in digital asset related activities and the ability for banks to use blockchain technologies to improve their services.

This section details how banks[222] and credit unions (collectively, "depository institutions") are engaging with digital assets and outlines the prudential regulatory framework applicable to: (i) depository institutions engaging in digital asset activities or offering banking services to digital asset firms; and (ii) digital asset firms interested in offering bank-like services. It then makes recommendations that would help ensure depository institutions can continue to innovate to meet customer demand for engagement in digital asset markets and use DLT throughout this new opportunity for growth.

Bank Engagement with Digital Assets

Banks have primarily engaged with the digital assetindustry through: (i) providing core banking products and services to digital asset market participants; and (ii) facilitating customer access to digital asset markets through services such as custody,trade execution, and settlement. Due to general skepticism or concerns aboutrisk, banks were initially slow to engage with digital assets. However, interestin digital asset-related productlines accelerated in 2020 and 2021 as the broader digital asset market experienced a period of substantial price gains and opportunities to leverage DLT became more apparent. This was accompanied by the OCC's issuance of a series of interpretive letters toward the end of President Trump's first administration

related to the permissibility of certain digital asset activities, which added some regulatory certainty.[223] However, in 2022, a series of market events, including a substantial decrease in the value of digital assets, [224] and the onset of the Biden Administration's Operation Choke Point 2.0 impacted many banks' interestin pursuing orincreasing engagement with digital assets. Though banking agencies have steadily removed many ofthe previous regulatory impediments, certain areas ofregulatory uncertainty remain and need to be addressed.[225]

221 Brian Deese, Arati Prabhakar, Cecilia Rouse & Jake Sullivan, *The Administration's Roadmap to Mitigate Cryptocurrencies' Risks*, The White House (Jan. 27, 2023), https://bidenwhitehouse.archives.gov/nec/briefing-room/2023/01/27/the-administrations-roadmap-to-mitigate-cryptocurrencies-risks. 222 As used in this chapter of the report, "banks" broadly refers to and includes insured depository institutions and OCC-chartered trust banks. 223 OCC, Interpretive Letter No. 1170, Authority of a National Bank to Provide Cryptocurrency Custody Services for Customers (July 22, 2020), https://occ.gov/topics/charters-and-licensing/interpretations-and-actions/2020/int1170.pdf; OCC, Interpretive Letter No. 1172, OCC Chief Counsel's Interpretation on National Bank and Federal Savings Association Authority to Hold Stablecoin Reserves (Sept. 21, 2020), https://occ.gov/topics/charters-and-licensing/interpretations-and-actions/2020/int1172.pdf; OCC, Interpretive Letter No. 1174, OCC Chief Counsel's Interpretation on National Bank and Federal Savings Association Authority to Use Independent Node Verification Networks and Stablecoins for Payment Activities (Jan. 4, 2021), https://occ.gov/topics/charters-and-licensing/interpretations-and-actions/2021/int1174.pdf.

224 *See* Financial Stability Oversight Council (FSOC), Report on Digital Asset Financial Stability Risks and Regulation 27 (2022), https://home.treasury.gov/system/files/261/FSOC-Digital-Assets-Report-2022.pdf (noting that "... the substantial decline in crypto-asset prices during late 2021 and early 2022 reportedly coincided with some key market developments" and throughout the report referring to the failure of the hedge fund Three Arrows Capital, the collapse of the TerraUSD stablecoin and associated liquidation of the Luna Foundation Guard's bitcoin holdings, and the bankruptcies of Celsius and Voyager Digital). Additionally, the cryptocurrency exchange FTX filed for bankruptcy in November 2022. FTX Trading Ltd., Form 201, No. 22-11068-JTD (D. Del. Nov. 11, 2022).

225 *See* FSOC, *supra* note 224, at 18 (noting that "some banks have indicated publicly that they have interest in offering crypto-asset products and services but are waiting on regulatory clarity before doing so.").

Current Products and Services

Banks provide a variety of traditional banking products and services to digital asset firms such as commercial deposit accounts, loans, and capital markets advisory services. Some banks also offer other services, directly or indirectly, related to the trading, settlement, and custody of native digital assets, though uptake is currently limited. The use of third parties commonly serves as a vehicle for banks to leverage new technologies, access greater expertise for a particular activity, or enter new marketplaces. Community banks in particular often find that they can harness the resources of third parties to leverage emerging technologies and create new opportunities for the bank and its customers. In recent years, banks have explored a range of business lines through external relationships, including custody services, facilitating customer purchases and sales of digital assets, loans involving digital assets, and DLT payments networks. Additionally, some banks and digital asset market participants partner to offer hybrid traditional banking and digital asset products, such as debit or credit cards that provide digital asset rewards.

Adopting new technologies or offering new products or services are business decisions. Regulatory guidance from the OCC, FDIC, and FRB (collectively, the "Banking Agencies") would be helpful for banks to evaluate digital asset activities. In any event, it is imperative that any banking regulatory framework not reflect a regulatory preference for a particular technology or sector so that banks may determine the mix of products and services to offer based on their business strategies and risk management capabilities and consistent with applicable law.

Traditional (Core) Banking Services

Depository institutions play a valuable role in providing traditional banking services to digital asset market

participants. Access to traditional banking services (e.g., deposit accounts, payments, lending) is essential for any company or individual. It enables them to manage cash flows, pay employees and vendors, and conduct their operations efficiently. For digital asset firms, maintaining a reliable banking relationship provides them with the critical infrastructure to interact with the broader economy. Those core banking services are provided to digital asset firms by depository institutions in accordance with their individual risk appetites and business decisions, while operating within a regulated framework.

In the past, regulatory uncertainty contributed to reduced availability or stability of banking relationships for firms and individuals operating in digital asset markets. However, regulators have recently reiterated that banks are neither prohibited nor discouraged from providing banking services to customers of any specific class or type, as permitted by law or regulation. Therefore, banks themselves should make risk-based business decisions regarding each potential customer relationship based on the banks' specific risk management capabilities and tolerances.

Payments

Some banks are seeking to harness DLT to facilitate faster payments. For example, some banks have formed consortia to establish new networks leveraging DLT for low-cost, real-time payment capabilities available 24/7/365.[226] Such DLT-based solutions, sometimes relying on third-party providers, may also have the capability to facilitate smart contracts that can extend functionality. Other banks are utilizing DLT to facilitate payments within a banking organization. Some are exploring leveraging public blockchains.

226 *See, e.g.*, *Regulated Settlement Network Proof-of-Concept*, Securities Industry and Financial Markets Association, https://www.sifma.org/resources/general/regulated-settlement-network-proof-of-concept (last visited July 13, 2025); *Big Banks Explore Interoperable Stablecoin*, PYMNTS.com (May 23, 2025), https://www.pymnts.com/cryptocurrency/2025/big-banks-eye-consortium-backed-stablecoin-to-counter-fintech-threat; *How It Works*, Fnality, https:// fnality.com/how-it-works (last visited July 13, 2025).

Tokenization

Tokenization entails bringing traditional products and services onchain using DLT. This enables both the bank and its clients to benefit from capabilities that are commonly implemented on distributed ledgers, such as the potential to encode rules or conditions into the tokenized assets and liabilities themselves (i.e., programmability). Tokenization has the potential to transform execution, settlement, and other banking activities that could benefit from these efficiencies.[227] Clarity within the regulatory perimeter may contribute to dislocation of legacy system intermediaries and traditional financial market infrastructures (FMIs).

When deciding which traditional products to tokenize, banks and their clients generally appearto be focusing on the financial activities they view as mostreliant on inefficient market structures and on products that align with their core competencies. Although tokenization is occurring across all financial services, bank tokenization projects garnering the most public attention are tokenized deposits, digital foreign exchange (FX), custody of tokenized securities, tokenized repurchase agreements, and tokenized private funds.[228] Tokenization also presents an opportunity for banks to bring loans onchain, potentially improving operational efficiency and access to capital,[229] especially forlending to small and medium-sized enterprises (including by community banks).

Tokenized Deposits

Tokens may represent a range of different kinds of assets and liabilities, including commercial bank deposits. Banks are generally permitted to tokenize deposits in the U.S., as tokenization can be viewed as a form of technology to record bank deposits;[230] nonetheless, further clarity on this point from the Banking Agencies would be helpful.[231]

A tokenized deposit may offer the familiarity and safety of a bank deposit, with the added functionality of instantaneous settlement of DLT. Depository institutions are actively exploring and deploying use cases; some banks have used tokenization and tokenized deposits to facilitate 24/7, real-time, intra-bank transfers or have expressed interest in pursuing the tokenization of deposits. These improvements to internal systems may enable more efficient transfers of funds, as well as new types of financial products. Others are seeking to use tokenized deposits to facilitate transfers among trusted participants in a network. For example, as discussed below, some are pursuing tokenized deposits to facilitate wholesale, cross-border payments.

Tokenization of deposits, like any novel technology, may raise certain questions regarding practical implementation and broader impact on the banking system. For example, banks should establish certainty for

227 Many of the product designs under development have the potential to integrate features from different sources. For example, a bank-owned distributed ledger platform could leverage components and solutions developed in house or by third-party providers. Likewise, a bank may decide to tokenize its products through white-label offerings on third-party platforms. Finally, a bank could choose to provide services to clients through connectivity to a DeFi FMI platform using dApps. A quality known as "composability," similar to but more expansive than mere interoperability, enables clients or customers to design new or unique financial products using off the shelf templates and tools, presenting both opportunities and risks for firms.

228 *See* Oliver Wyman & J.P. Morgan Chase & Co., Deposit Tokens: A Foundation for Stable Digital Money (2022), https://www.jpmorgan.com/kinexys/documents/deposit-tokens.pdf; Citigroup, Bringing Traditional Assets to Digital Networks: Exploring the Tokenization of Private Markets (2024), https://www.citigroup.com/rcs/citigpa/storage/public/Fund-Tokenization-Summary-Report.pdf; *Citi and Fidelity International Demonstrate Tokenized Money Market Fund and Digital Foreign Exchange Swap Solution*, Citigroup (Nov. 4, 2024), https://www.citigroup.com/global/news/press-release/2024/citi-and-fidelity-international-demonstrate-tokenized-money-market-fund-and-digital-foreign-exchange-swap-solution; *Reinventing Asset Servicing with Distributed Ledger Technology*, HSBC (May 20, 2024), https://www.gbm.hsbc.com/en-gb/insights/market-and-regulatory-insights/reinventing-asset-servicing-with-distributed-ledger-technology; *BNP Paribas Trades Intraday Repo on J.P. Morgan's Onyx Digital Assets Platform*, BNP Paribas (May 16, 2022), https://globalmarkets.cib.bnpparibas/bnp-paribas-trades-intraday-repo-on-j-p-morgans-onyx-digital-assets-platform-2.

229 *See Tokenization in Financial Services: Delivering Value and Transformation*, PwC (Mar. 11, 2024), https://www.pwc.com/us/en/tech-effect/emerging-tech/tokenization-in-financial-services.html ("Historically illiquid assets, such as private credit and private equity, can also be viable tokenization candidates. In the roughly $1.5 trillion private credit market, for example, it can take a tremendous amount of time and effort to match buyers and sellers. When private credit starts utilizing tokenization, lenders can "fractionalize" loans, making them into a variety of sizes, increasing the pool of potential borrowers.").

230 *See* Acting Chairman Hill, *supra* note 217 ("From the FDIC's perspective, we should provide certainty that 'deposits are deposits, regardless of the technology or recordkeeping deployed.'") (quoting Vice Chairman Travis Hill, FDIC, Speech at Mercatus Center, Banking's Next Chapter? Remarks on Tokenization and Other Issues (Mar. 11, 2024), https://www.fdic.gov/news/speeches/2024/spmar1124.html).

231 Whether any particular tokenized deposit product meets the statutory or regulatory definitions of "deposit" for purposes under 12 U.S.C. § 1813(l) or 12 C.F.R. pt. 204 (2025) (commonly referred to as Regulation D) depends on a fact-specific analysis of the product.

their customers regarding the ability to transfer tokenized deposits. Additionally, banks and their customers must have confidence in the reliability and security of the underlying technology, and in the privacy of any confidential information shared when making a payment. Further, if there are many different ledgers, banks must consider how these ledgers interact or interoperate so that customers are able to transfer value freely.[232] Finally, programmability associated with tokenized deposits may increase the speed and automation of transactions, which may have an ancillary effect of increasing the speed of, and herding behavior leading to, bank runs. Conversely, programmability could also be used to introduce frictions into the transaction or settlement processes to reduce the speed of bank runs or otherwise provide incentives to mitigate the risk of herding behavior.[233]

Payments showcase how stablecoins[234] and tokenized bank deposits can be used for the same general purpose but differ significantly in implementation and legal treatment. Both stablecoins and tokenized deposits could be used as means of payment and operate on the same underlying technology. However, tokenized deposits are intended to evidence a bank's deposit liability and a holder's deposit claim against a regulated bank as recorded on a digital ledger. Bank deposits (including tokenized deposits) are supported by the bank's balance sheet and therefore can be subject to federal deposit insurance. Additionally, in the event of insolvency, the disposition of bank deposits would be addressed through receivership, which features special rules for deposit claims, rather than through bankruptcy proceedings. Stablecoins, on the other hand, may represent a liability of a bank subsidiary or nonbank counterparty or a claim on reserve assets. Certain customers and counterparties may value the added security of tokenized deposits, while others may value the full reserve based nature of certain stablecoins and their currently wider interoperability and acceptance within

the digital asset ecosystem.

Digital Asset Custody

As the digital asset market has grown, there has been an increasing demand for trusted institutions to provide custody services for digital assets, including safekeeping (e.g., controlling the cryptographic keys of customers' digital assets, transaction processing, and settlement).[235] Depository institutions have long provided custody services for a wide variety of physical and electronic assets, including assets that are unique and hard to value. As digital assets generally consist of entries on distributed ledgers, providing custody typically entails maintaining control of cryptographic keys (and potentially other sensitive information) used to transfer the assets on these ledgers. As in traditional custody services, customers may seek to engage the custodian to undertake ancillary services. In the digital asset context, ancillary services that customers may seek from a custodian include staking, facilitating digital asset lending, and DLT governance services. Depository institutions may provide custody services themselves or through sub-custodians to hold cryptographic keys or white-labeling digital asset custody platforms.

Currently, only a small number of banks offer digital asset custody, with a focus primarily on institutional customers. Several factors likely contributed to the relatively small number of banks that have decided to engage in this activity—most notably, the now-rescinded SEC SAB No. 121 to the extent such banks were (or were subsidiaries of) companies required to file certain periodic reports under applicable securities laws. The Biden Administration's Operation Choke Point 2.0 further contributed by creating additional procedural steps and costs to engage in digital asset activities alongside statements from federal banking regulators and the

232 The potential availability of multiple distributed ledgers or blockchains has some potential benefits, including offering redundancies in systems that improve system-wide resilience.

233 *See* Vice Chairman Hill, *Banking's Next Chapter? Remarks on Tokenization and Other Issues*, *supra* note 230 (discussing the potential for tokenization to exacerbate and mitigate risks of speed and intensity of bank runs).

234 *See* Chapter V.

235 *See* OCC, Interpretive Letter No. 1170, *supra* note 223, at 7, 8 (noting that providing custody services for digital assets falls within longstanding authorities to engage in safekeeping and custody activities, and that providing such services is permissible in both non-fiduciary and fiduciary capacities).

White House discouraging such engagement.[236] Digital asset companies interested in providing custody services as banks also faced strong difficulty in receiving bank charters from the OCC.[237] The need for custody expertise, competence with digital assets, and cybersecurity implications may also have reduced engagement by banks in such activities. Interest may also have been chilled by long-term volatility within the digital asset market and specific market events in 2022.[238] Finally, other factors that may have impacted a bank's decision to offer digital asset custody include competition (especially given that established digital asset companies frequently provide custody solutions—sometimes for little or no cost—and have substantial market share), significant capital requirements, the availability of self-custody options, the nascent nature of the technology in banking, and perceived risk implications. In July 2025, however, the Banking Agencies jointly reaffirmed the legal permissibility for banks to custody digital assets under existing laws, regulations, and risk-management principles without creating any new supervisory expectations.[239]

Facilitating Digital Asset Trading

Banks offer customers digital asset trading in varying forms. Some banks provide trade execution geared towards institutional and high net worth customers interested in gaining exposure to certain digital assets, supplementing custody services offered. Banks interested in offering retail customers exposure to digital asset markets may seek to provide these services through a third party. This simplest form of this arrangement enables bank customers to access the third party's digital asset trading service through the bank's website or app. In some cases, this falls within a banking organization's finder authority, which generally encompasses a bank bringing together parties to a transaction that the parties themselves negotiate and execute.[240] Other

types of arrangements related to digital asset trading may not fall within such authority,[241] but may, depending on the facts of the arrangement, fall under other authorities or require additional regulatory approvals.

A bank's role in such an arrangement depends on the relationship. In certain cases, it may include providing a variety of the third party's disclosures and statements to customers, providing customer service and complaint resolution, and performing requisite transaction compliance functions for the third party. Banks may receive a portion of the transaction fees paid by their customers and pay fees to the third party. Several banks have expressed an interest in expanding trade facilitation services. However, very few banks are currently using their finder authorities to provide digital asset trading to their customers.

Digital Asset-Related Lending

Some banks have entered into business arrangements to extend credit in transactions that involve digital assets. Examples include loans secured by digital assets or digital asset mining equipment, or loans used to fund the borrower's digital asset-related operations. While loan structures vary, such lending generally has unique credit administration considerations compared to traditional lending, including perfecting a security interest in digital asset collateral or providing for self-execution of loan terms. As such, banks looking to offer this line of business often engage a third party to custody collateral, provide valuations, manage margin calls, develop smart contracts, or provide other services as appropriate.

Digital asset-related lending activities by banks has so far been limited. Several factors likely contributed to this low interest, including the Biden Administration's Operation Choke Point 2.0, regulatory uncertainty, and

236 *See supra* note 221; *infra* notes 266-270.
237 *See supra* note 102.
238 *See supra* note 224.
239 Crypto-Asset Safekeeping by Banking Organizations, *supra* note 220.
240 *See, e.g.*, 12 C.F.R. § 7.1002 (2025) (national bank and federal savings association acting as finder); 12 C.F.R. § 225.86(d)(1) (2025) (financial holding company acting as finder).
241 For example, an arrangement under which a bank purchased digital assets as agent or principal or negotiated a purchase or sale may be inconsistent with a bank's finder authority. Finders bring together interested parties for a transaction that the parties themselves negotiate and execute.

difficulties managing volatility of valuations (both for digital assets and mining equipment). However, as digital asset markets continue to mature and bank customers increasingly hold digital assets, interest in using those assets as collateral is likely to increase.

Current Regulatory Framework

Federal law provides the Banking Agencies with authorities related to: (i) the supervision and regulation of banks, including the activities they can engage in and applicable requirements; (ii) the examination of banks to ensure compliance with applicable laws and regulations; and (iii) the imposition of corrective actions for unsafe or unsound practices or violations of law or regulation. In implementing federal law, the Banking Agencies may adopt rules and regulations to achieve the law's objectives and have also issued guidance, policy statements, and other supervisory directives to provide further direction to banks and to provide transparency and direction on how activities will be supervised.

In adapting the current banking regulatory framework to incorporate digital assets, it is imperative that the Banking Agencies employ a technology-neutral approach. Technological transformation does not necessarily alter the risk profile of an activity, and the same business presenting the same risk should be governed by the same rules. Banks should be able to engage in permissible digital asset activities in a safe and sound manner without prior regulatory approval or notice. Further, the Banking Agencies should monitor banks' digital asset activities through an appropriate supervisory process.

Legal Permissibility

Banks and their holding companies are subject to limitations on what types of activities they may conduct. The National Bank Act (NBA) generally defines the permissible activities for national banks and is administered by the OCC. The OCC's determination of whether a new activity is permissible for a national bank often involves consideration of whether that activity is part of, or incidental to, the "business of banking" under 12 U.S.C. § 24.[242]

One of the clearest benefits of the U.S. dual banking system, in which banks can be chartered at either the state or federal level, is the ability for states to "serve as laboratories for innovation,"[243] which has resulted in state banks "[taking] the lead in safe and sound product innovations, including variable-rate mortgages and home equity loans."[244] The OCC itself has stated that "[s]tate banking does not deliver the benefits of having separate state systems serve as 'laboratories' if state bank powers simply copycat national bank powers."[245] Nonetheless, since 2023, the permissible activities engaged in as principal by state non-member banks[246] and state member banks[247] are generally limited to those permitted under the NBA as interpreted by the OCC.

242 For federal savings associations, the permissibility of an activity typically depends on the Home Owners' Loan Act, 12 U.S.C. § 1461 et seq. 243 OCC, National Banks and the Dual Banking System 8, 9 (Sept. 2003), https://www.occ.gov/publications-and-resources/publications/banker-education/files/pub-national-banks-and-the-dual-banking-system.pdf.

244 Julie L. Stackhouse, *Why America's Dual Banking System Matters*, Federal Reserve Bank of St. Louis (Sept. 18, 2017), https://www.stlouisfed.org/on-the economy/2017/september/americas-dual-banking-system-matters.

245 OCC, *supra* note 243, at 11.

246 Section 24 of the Federal Deposit Insurance Act generally prohibits all insured state banks (member and non-member) and their subsidiaries from engaging as principal in activities that are not permissible for national banks and their subsidiaries, unless (i) the FDIC has determined that the activity would pose no significant risk to the Deposit Insurance Fund; and (ii) the state bank is, and continues to be, in compliance with applicable capital standards. 12 U.S.C. § 1831a. *See also* 12 U.S.C. § 1831e with respect to activities of state savings associations. Additionally, under certain circumstances, the FDIC may approve additional activities for insured state-chartered banks. *See* 12 C.F.R. § 362 (2025).

247 Under Section 9(13) of the Federal Reserve Act, a state member bank retains its full charter and statutory rights as a state bank and may continue to exercise all corporate powers granted it by the state in which it was created. However, the Board may limit the activities of state member banks and their subsidiaries in a manner consistent with Section 24 of the Federal Deposit Insurance Act. *See supra* note 246. The Board issued a policy statement, which it ultimately codified in Regulation H, interpreting Section 9(13) of the Federal Reserve Act to create a rebuttable presumption against permissibility of "novel and unprecedented" activities, including crypto-asset-related activities. Policy Statement on Section 9(13) of the Federal Reserve Act, 88 Fed. Reg. 7848 (Feb. 7, 2023) (codified at 12 C.F.R. pt. 208 (2025)).

In February 2023, as a continuation ofthe Biden Administration's Operation Choke Point 2.0 efforts to shut down interestfrom state member banks in engaging in digital asset-related activities and other "novel and unprecedented" activities, the FRB issued a policy statement interpreting Section 9(13) of the Federal Reserve Actto "set out a rebuttable presumption thatit will exercise its discretion underthat provision to limit state member banks to engaging as principal in only those activities that are permissible for national banks—in each case, subjectto the terms, conditions, and limitations placed on national banks with respectto the activity— unless those activities are permissible for state banks by federal statute or under part 362 ofthe Federal Deposit Insurance Corporation's regulations."[248] State member banks interested in engaging in such activities are now required to demonstrate to the FRB a "clear and compelling rationale" for permitting the activities and that the bank has "robust plans for managing the risks" of such activities in accordance with principles of safe and sound banking. The FRB then revised Regulation H, which defines the membership requirements for state-chartered banks,to incorporate the 2023 policy statement, effectively codifying the rebuttable presumption into law.[249]

As a consequence, the activities that the OCC has authorized for national banks, if permitted under state law, generally represent the full breadth of activities in which a state member bank may engage as principal without limitation under Section 9(13), contrary to the longstanding tenet that the dual banking system should promote innovation in new banking products on the state level. The FRB's utilization of Section 9(13) and its discretionary powers under §208.3(d)(2) of Regulation H has resulted in a de facto prohibition by state member banks from engaging in most digital asset related activities.

At the organizational level, the Bank Holding Company Act, which is administered by the FRB, generally governs the permissibility of the activities of bank holding companies (BHCs) and financial holding companies (FHCs).[250] The BHC Act primarily restricts the activities of BHCs and their subsidiaries to activities that are closely related to banking.[251] In addition, BHCs that elect to be treated as FHCs (per the Gramm-Leach-Bliley Act) can engage in a broader range of nonbanking activities that are "financial in nature," "incidental to a financial activity," or "complementary to a financial activity."[252] Any significant acquisitions or expansions into new activities by BHCs and FHCs generally require FRB approval.

In July 2020, the OCC issued Interpretive Letter No. 1170 that concluded that national banks and federal savings associations (FSAs) may provide digital asset custody services, including the safekeeping of cryptographic keys for customers.[253] In September 2020, the OCC issued Interpretive Letter No. 1172 that concluded that national banks and FSAs may hold deposits that serve as reserves backing stablecoins.[254] Then, in January 2021, the OCC issued Interpretive Letter No. 1174 that concluded that national banks and FSAs may use DLT and related stablecoins to conduct bank-permissible payment activities.[255] Later, the OCC issued Interpretive Letter No. 1179, which set forth a supervisory non-objection process for engaging in the activities described in Interpretive Letters Nos. 1170, 1172, and 1174.[256] In March 2025, the OCC issued Interpretive Letter No. 1183, which rescinded Interpretive Letter No. 1179 thereby eliminating the supervisory non-objection

248 88 Fed. Reg. 7848, *supra* note 246.
249 12 C.F.R. § 208.112 (2025).
250 The Home Owners' Loan Act governs the activities of savings and loan holding companies. 12 U.S.C. § 1467a(c).
251 This includes extending credit and related activities, leasing personal or real property, trust company functions, financial and investment advisory activities, agency transactional services for customer investments (e.g., securities brokerage), management consulting, certain insurance activities, and data processing.
252 12 U.S.C. § 1843(k)(1). For example, FHCs may, among otherthings, act as finderin bringing together one or more buyers and sellers of a product or service; engage in merchant banking and certain insurance underwriting activities; and engage in underwriting, dealing in, or making a marketin securities.
253 OCC, Interpretive Letter No. 1170, *supra* note 223.
254 OCC, Interpretive Letter No. 1172, supra note 223.
255 OCC, Interpretive Letter No. 1174, supra note 223.
256 OCC, Interpretive Letter No. 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 (Nov. 18, 2021), https://www.occ.treas.gov/topics/charters-and-licensing/interpretations-and actions/2021/int1179.pdf.

process described in that letter. Interpretive Letter No. 1183 also reaffirmed that the activities addressed in Interpretive Letters Nos. 1170, 1172, and 1174 are permissible.[257] In May 2025, the OCC issued Interpretive Letter No. 1184, which confirmed that national banks and FSAs could buy and sell digital assets held in custody at the customer's direction and outsource bank-permissible digital asset activities to a third party.[258] Finally, in July 2025, the Banking Agencies issued a joint statement reaffirming the legal permissibility for banks to custody digital assets under the existing regulatory framework without creating any new supervisory expectations.[259]

In November 2021, the Banking Agencies issued a joint statement outlining plans to provide greater clarity on whether certain activities related to digital assets conducted by banks are legally permissible and to describe expectations for safety and soundness, consumer protection, and compliance with existing laws and regulations related to a number of digital asset related activities, specifically highlighting custody, facilitation of customer purchases and sales, digital asset collateralized lending, stablecoin activities, and holding digital assets on balance sheet. However, under the Biden Administration, the Banking Agencies did not carry out those plans to provide guidance specific to those digital asset activities, and as mentioned above, the Federal Reserve's policy statement on Section 9(13) and corresponding revisions to Regulation H further complicated the degree to which state member banks could engage in digital asset-related activities.

Therefore,there remains significant outstanding uncertainty regarding the permissibility of digital asset-related activities atthe bank level, especially beyond those addressed in OCC Interpretive Letters Nos.1170,1172,1174, 1183, and 1184, and outside the bank chain within a BHC/FHC structure. For example, banks are interested in acquiring and using digital assets to pay transaction fees (e.g., gas fees) to conduct

bank-permissible activities on public blockchains. Likewise, banks are seeking clarity on whether and how they may purchase and sell digital assets as riskless principals for customers and whether banks may make markets in digital assets. Similarly, banks are seeking clarity regarding their authority to act as finders and lenders in the context of digital asset-related activities, and whether some activities are permissible only atthe BHC/FHC level.

Depository Institution and Market Participant Concerns

A clear regulatory framework is required to ensure that depository institutions can continue to innovate responsibly to facilitate customer engagement with digital assets and to use digital asset technology in a safe and sound manner that complies with applicable laws and regulations. Any regulatory framework should be derived from a clear statutory basis and be efficient and fair. Therefore, it is essential that the Banking Agencies ensure that they employ a technology-neutral approach to bank regulation and supervision when incorporating digital assets into the current banking regulatory framework. As a policy matter, and from the perspectives of efficiency and competition, it could be detrimental to innovation in the financial system for the Banking Agencies to treat decentralization and permissionless infrastructure as categorically negative given the potential benefits of this technology. While the regulators have retracted much of the Biden Administration's approach to digital asset supervision that may have hampered banks' ability to engage with digital assets, additional work is needed to address many of the remaining concerns expressed by depository institutions.

Depository institutions have expressed many concerns regarding the current regulatory framework, most notably:

- A lack of legal clarity on whether banks can offer certain digital asset-related products and services and use DLT technology in certain areas. Specifically, banks have asked for further clarity as to whether they may use public, permissionless blockchains now that the effective prohibition of such use under the Biden

257 OCC, Interpretive Letter No. 1183, *supra* note 216.
258 OCC, Interpretive Letter No. 1184, *supra* note 216.
259 Crypto-Asset Safekeeping by Banking Organizations, *supra* note 220.

Administration has been lifted.[260] Additionally, banks have asked for guidance on how they can safely and soundly engage in such activities.

- A lack of clear standards on safe and sound engagement with digital assets; the Banking Agencies have not ensured supervisory consistency and expertise in bank digital asset engagement.
- A lack of clear capital standards on balance sheet treatment for many digital assets and concern that the BCBS standards may not accurately reflect current risks.
- Difficulties reported by some digital asset market participants in either finding or maintaining banking services.
- A lack of clarity for eligible firms on the expectations and process for obtaining a bank charter or a Reserve Bank master account.

Recommendations

Relaunch agency crypto innovation efforts—as appropriate—to address outstanding bank activities.

- These efforts should prioritize providing clarity on the activities that banks are most interested in conducting with a clear process for considering other or new activities. The objectives would be

to:

- ◆ Clarify or expand the recognized, permissible digital asset activities in which banks may engage, consistent with applicable law;
- ◆ To the extent possible, and consistent with applicable law, ensure parity in permissibility between bank charter types; and
- ◆ Clarify supervisory expectations on safe and sound conduct that protects consumers and is compliant with applicable laws and regulations in bank engagement with digital assets, private and permissionless blockchains, tokenized deposits, and where to conduct principal bank activities (e.g., in the insured depository institution or the holding company).

- The initial activities and topics to consider include:
  - ◆ *Custody of Digital Assets.* While the Banking Agencies have clarified permissibility and certain risk management considerations,[261] it could be beneficial to provide additional guidance on technical best practices.
  - ◆ *Third Parties.* While the Banking Agencies have clarified the permissibility of using third parties as sub-custodians,[262] it may be beneficial to ensure any additional guidance on permissibility or risk management for other digital asset activities reiterates the ability to use third parties as infrastructure providers or for other digital asset services.
  - ◆ *Holding Stablecoin Reserves as Deposits.* While the OCC has clarified permissibility,[263] it could be beneficial to offer additional guidance now that GENIUS has been enacted.
  - ◆ *Principal Activities.* Provide clarity on the permissibility for depository institutions to hold digital assets on their balance sheet and any associated safety and soundness concerns.[264]

260 *See* Acting Chairman Hill, *supra* note 217 ("One specific area that merits attention is the use of public, permissionless blockchains by banks. Other jurisdictions have allowed banks to interact with public chains for many years, but the U.S. banking agencies have effectively prohibited it . . . . The banking agencies will need to formally revisit the January 2023 and February 2023 interagency guidance and develop durable standards for the responsible use of public chains, as well as other activities implicated by the guidance.")

261 Crypto-Asset Safekeeping by Banking Organizations, *supra* note 220; OCC, Interpretive Letter No. 1170, *supra* note 223; OCC, Interpretive Letter No. 1183, *supra* note 216; OCC, Interpretive Letter No. 1184, *supra* note 216.

262 Crypto-Asset Safekeeping by Banking Organizations, *supra* note 220; OCC, Interpretive Letter No. 1170, *supra* note 223; OCC, Interpretive Letter No. 1184, *supra* note 216.

263 OCC, Interpretive Letter No. 1172, *supra* note 223; OCC, Interpretive Letter No. 1174, *supra* note 223; OCC, Interpretive Letter No. 1183, *supra* note 216. 264 Banks have also expressed interest in holding and using small amounts of cryptocurrency to pay transaction or gas fees for customers and in conducting riskless principal cryptocurrency transactions.

- ◆ *Pilots.* Clarity is needed on the ability for depository institutions to participate in pilots and experiments related to digital assets.
- ◆ *Tokenization.* Provide clear risk-based guidelines that consider underlying risk and asset features to determine the permissibility of bank tokenization activities, including tokenization of deposits. ◆ *Permissionless Blockchains.* Provide clarity regarding the use of permissionless blockchains that ensures a technology-neutral approach focusing on underlying risks of the activity or technology versus using technology alone as a proxy for risk.

Encourage innovation in banking technologies and products by state-chartered banks.

- The FRB should rescind the 2023 Section 9(13) Policy Guidance and 12 C.F.R. § 208.112 (which effectively codifies the Policy Guidance into Regulation H), to ensure that state member banks are permitted to explore innovative banking technologies and products.

Develop guidance and best practices to support banks and supervisors that is technically sound and principles-based.

- Risk management principles and best practices described in existing agency issuances generally provide

flexible guidance for banking organizations' considerations that can apply to the safe and sound implementation of innovative technologies and products, including those related to digital assets and DLT.[265] Nonetheless, it is important that agency examination teams and banks are properly equipped to adopt current risk management principles to digital asset technologies.

- This could involve engagement with NIST and others to identify applicable standards or best practices that could be used in guidance for some digital asset activities such as providing digital asset custody services, ensuring compliance with applicable AML/CFT obligations (see Chapter VI, which discusses the AML specific regulatory duties for digital assets for more details), or managing cyber risks particular to digital assets.
- This could also include best practices or standards applicable to banks' use of third parties in the provision of digital asset services.
- Finally, the Banking Agencies and state regulators should ensure that their examination teams are adequately educated on issues related to digital assets and the consistent application of best practices and standards across institutions.

Supervision

Bank supervisors should expect bank risk management processes to be applied based on risk, with the intensity and rigor of risk management corresponding to, among other things, the complexity, criticality, and magnitude of the technological change or new activity. Banks considering the adoption of new technologies should consider their overarching business strategy, policy objectives, and existing risk management and compliance frameworks when identifying whether and how existing controls may be adapted and supplemented. Similarly, the Banking Agencies should examine banks' activities from a technology-neutral approach, focusing on such activities' material risks and the banks' abilities to manage such risks.

While certain digital asset activities were legally permissible in the past, many banks were deterred in part to the Biden Administration's supervisory framework governing such activities. Following the issuance of the OCC's interpretive letters in 2020 and 2021 clarifying the permissibility of certain digital asset activities at the end of President Trump's first administration, the Banking Agencies subsequently effected notification

265 *See, e.g.*, OCC, Bulletin 2017-43, New, Modified, or Expanded Bank Products and Services: Risk Management Principles (Oct. 20, 2017), https://www.occ.treas.gov/news-issuances/bulletins/2017/bulletin-2017-43.html.

and non-objection processes for banks seeking to engage in digital asset activities and issued statements highlighting heightened risks associated with certain digital asset activities.

As noted above, in November 2021, the OCC issued Interpretive Letter No. 1179 which set forth a supervisory non-objection process for engaging in certain crypto-related activities;[266] in April 2022, the FDIC issued Financial Institution Letter 16-2022 requesting that supervised institutions notify the FDIC prior to engaging in crypto-related activity;[267] and in August 2022, the FRB issued SR Letter 22-6 requesting that supervised institutions notify Federal Reserve supervisors prior to engaging in crypto-related activity.[268] In January 2023, the Banking Agencies jointly issued a statement on digital asset risks to banking, asserting that business models that are concentrated in digital assets raise significant safety and soundness concerns and that issuing or holding as principal digital assets that are issued, stored, or transferred on an open, public, and/or decentralized network is highly likely to be inconsistent with safe and sound banking practices.[269] In February 2023, the Banking Agencies jointly issued a statement on the liquidity risks to banks presented by certain sources of funding from digital asset related entities.[270]

The Biden Administration's approach severely curtailed bank engagementin digital assets. However, as previously mentioned,the Banking Agencies rescinded their notification and non-objection processes in early 2025 to clarify that banks may engage in permissible digital assetrelated activities withoutreceiving prior regulatory approval.[271] The Banking Agencies also withdrew the January 2023 and February 2023 joint statements to provide further clarity that banks may engage in permissible digital asset activities and provide products and services to persons and firms engaged in digital asset-related activities, consistent with safety and soundness and applicable laws and regulations.[272] Those series of actions have moved the supervision of bank digital assets activities back to the regular supervisory process. Nonetheless, some banks have indicated that additional guidance, such as on best practices, could provide additional clarity on supervisory expectations forrisk managementrelated to specific aspects of digital asset activities (e.g., custody, BSA/AML, and cyber security).[273]

Recommendations

Clarify the role of supervisors and banks in offering banking services to potential customers.

- The Banking Agencies should ensure that existing and new best practices or guidance on risk management and bank engagement are technology-neutral and that expectations regarding offering banking services do not discriminate against lawful businesses solely due to their industry. For example, OCC Bulletin 2014-58: Banking Money Services Businesses: Statement on Risk Management, which makes clear that the OCC expects OCC-regulated banks to assess the risks posed by an MSB customer on a case-by-case basis rather than to consider all MSBs high risk, could be extended, and the FRB and FDIC could issue similar guidance.[274]

266 OCC, Interpretive Letter No. 1179, *supra* note 256.
267 FDIC, FIL 16-22, Notification of Engaging in Crypto-Related Activities (Apr. 7, 2022), https://www.fdic.gov/news/inactive-financial-institution-letters/2022/ fil22016.html.
268 FRB, SR 22-6, Engagement in Crypto-Asset-Related Activity by Federal Reserve-Supervised Banking Organizations (Aug. 16, 2022), https://www.federalreserve.gov/newsevents/pressreleases/files/bcreg20250424a3.pdf.
269 Joint Statement on Crypto-Asset Risks to Banking Organizations, *supra* note 219.
270 Joint Statement on Liquidity Risks to Banking Organizations Resulting from Crypto-Asset Market Vulnerabilities, *supra* note 219. 271 *See* FDIC Press Release, *supra* note 215; FRB Press Release, *supra* note 218; Press Release, OCC, OCC Clarifies Bank Authority to Engage in Certain Cryptocurrency Activities (Mar. 7, 2025), https://www.occ.treas.gov/news-issuances/news-releases/2025/nr-occ-2025-16.html.
272 *See* Press Release, FDIC, Agencies Withdraw Joint Statements on Crypto-Assets (Apr. 24, 2025), https://www.fdic.gov/news/press-releases/2025/agencies withdraw-joint-statements-crypto-assets.
273 *See* Chapter VI.
274 *See* OCC, Bulletin 2014-58, Banking Money Services Businesses: Statement on Risk Management (Nov. 19, 2014), https://www.occ.gov/news-issuances/bulletins/2014/bulletin-2014-58.html.

- ◆ Notably, much work has already been done in in this area as the Banking Agencies withdrew previous guidance on bank engagement with digital assets that did not fully adhere to that principle.[275]
- ◆ Additionally, the removal of reputation risk as a basis for supervisory criticism by the Banking Agencies is also underway and should be finalized as soon as possible.[276]

Access to Providing Banking Services

Some digital asset firms that provide payments, lending, or custody services may consider obtaining a bank charter to provide additional services in a prudentially regulated environment and to reduce reliance on third party banks. Digital asset firms may consider a bank charter (including certain uninsured state or national charters) to gain strategic autonomy and cost efficiencies, allow better integration with the mainstream financial system, and gain regulatory credibility which could increase trust from both retail and institutional clients. Additionally, some firms may seek bank charters to obtain Federal Reserve Bank (Reserve Bank) master accounts and payment service access, which could reduce costs, delays, and counterparty risks in processing payments. These benefits could offer those digital asset firms a competitive advantage over other

digital asset firms and fintech companies, and a level playing field with traditional financial institutions.

Charters

A bank charter is a legal authorization that allows a legal entity to operate as a bank. Banks generally accept deposits, make loans, and provide other financial services such as payments, wealth management, custody, and currency exchange. While some charters (and relevant federal and state laws) permit banks to engage in all of these activities, some may be limited to a subset of commercial bank services. A bank also generally
meets the legal threshold for a Reserve Bank master account and payment services access,[277] and applicable laws may make an institution eligible to apply for FDIC insurance (but do not necessarily require it for some novel charters) and provide eligibility for other U.S. banking infrastructure. States may charter general-purpose commercial banks that must be federally insured before commencing operations; these state-chartered banks are regulated by both the state chartering authority and a federal regulator. The FRB is the primary federal regulator for state-chartered banks that are members of the Federal Reserve System (FRS), and the FDIC is the primary federal regulator for federally-insured state-charted institutions that are not members of the FRS. The OCC charters national banks and federal savings associations and is their primary federal regulator. The FDIC also has back up examination authority over insured banks for which either the OCC or FRB is the primary federal regulator.

Chartered banks are subject to, among other things, prudential regulation, capital and liquidity requirements, consumer protection laws, and regulatory supervision and enforcement. Chartering authorities may charter institutions that do not provide the full range of commercial bank services or that are not required to obtain deposit insurance. For example, certain banks engage in a more limited business model, such as special purpose credit-card banks or banks with activities limited to those of a trust company and activities related thereto. States may also charter depository institutions that have the authority to take deposits but are not required to obtain federal deposit insurance. Different resolution frameworks would apply as well. The activities undertaken by the institution determine the necessary type of charter, regulatory framework, and

275 *See* OCC, Bulletin 2025-2, Bank Activities: OCC Issuances Addressing Certain Crypto-Asset Activities (Mar. 7, 2025), https://occ.gov/news-issuances/bulletins/2025/bulletin-2025-2.html; FDIC Press Release, *supra* note 272.

276 The OCC and the Board have announced that they will no longer examine banks for reputation risk. *Supra* note 217. The FDIC is also "working on a rulemaking related to reputation risk that would prohibit FDIC supervisors from (1) criticizing or taking adverse action against institutions on the basis of reputational risk and (2) requiring, instructing, or encouraging institutions to close, modify, or refrain from offering accounts on the basis of political, social, cultural, or religious views." Acting Chairman Hill, *supra* note 217.

277 As explained in further detail below, the FRB has established guidelines for the Reserve Banks to use when evaluating whether to exercise their discretion to grant access to master accounts or payments services.