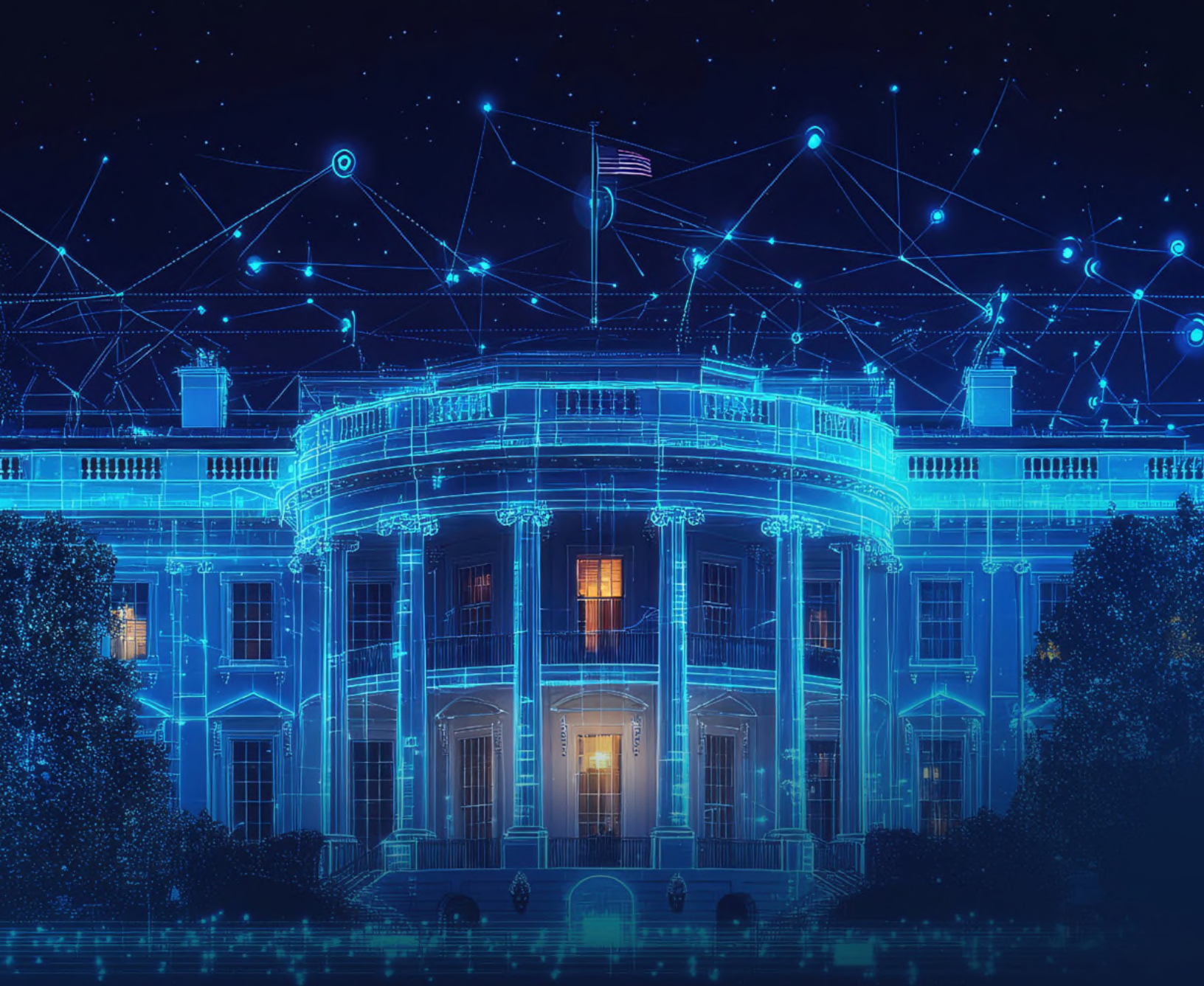


STRENGTHENING AMERICAN LEADERSHIP IN DIGITAL FINANCIAL TECHNOLOGY

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.

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 suggest that more than one in five Americans, or over 68 million people, own cryptocurrencies.[5] 82% of these investors believed June 2025 to be a good time to invest in 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 for this 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.

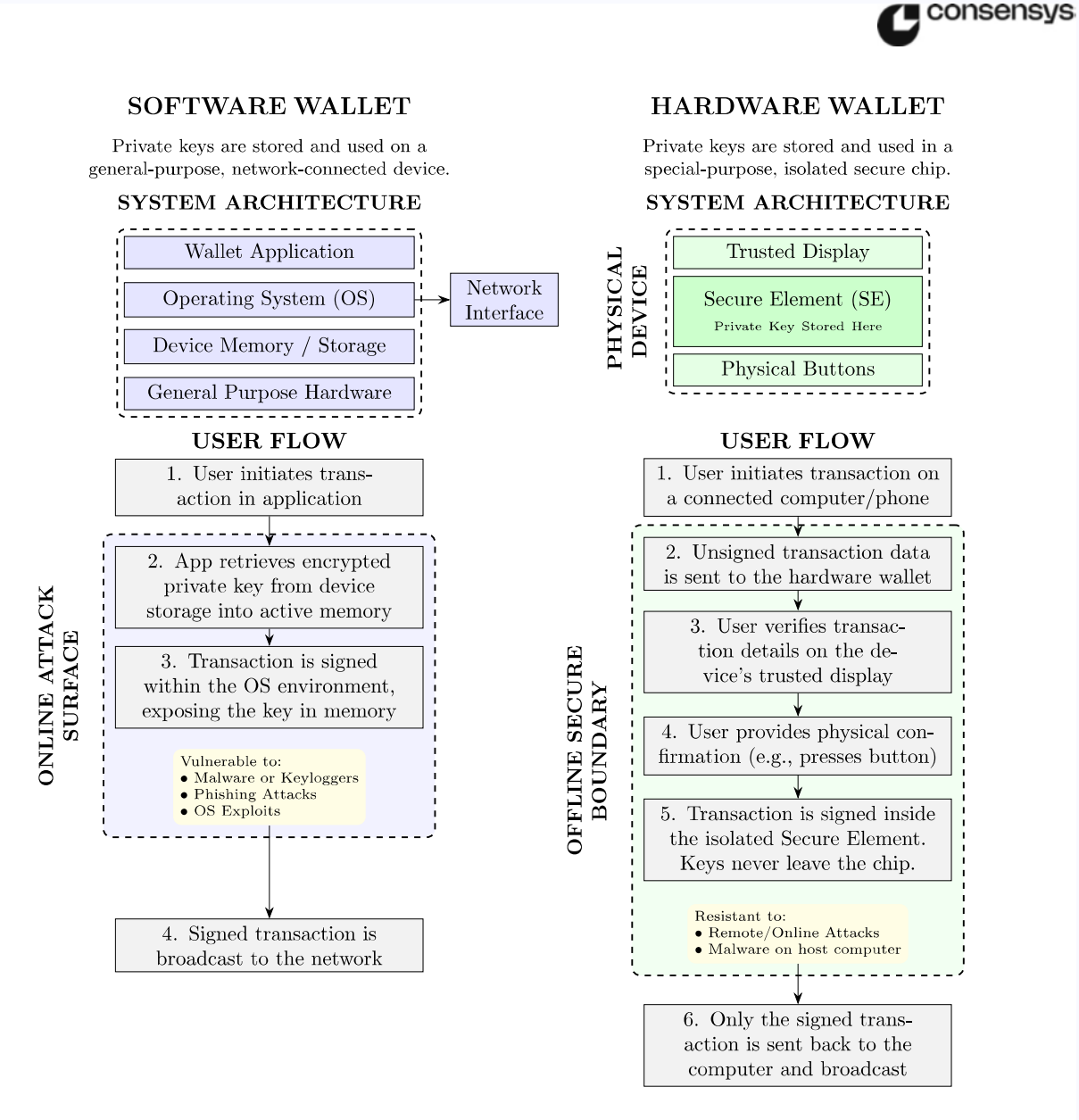
20 Consensus is the process by which all the participants in a blockchain network (e.g., Bitcoin) agree to the at-time state of the blockchain. This ensures (i) that all nodes have the same version of the ledger, and (ii) the integrity and security of the blockchain. *See* Kraken Learn Team, *What Is 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.

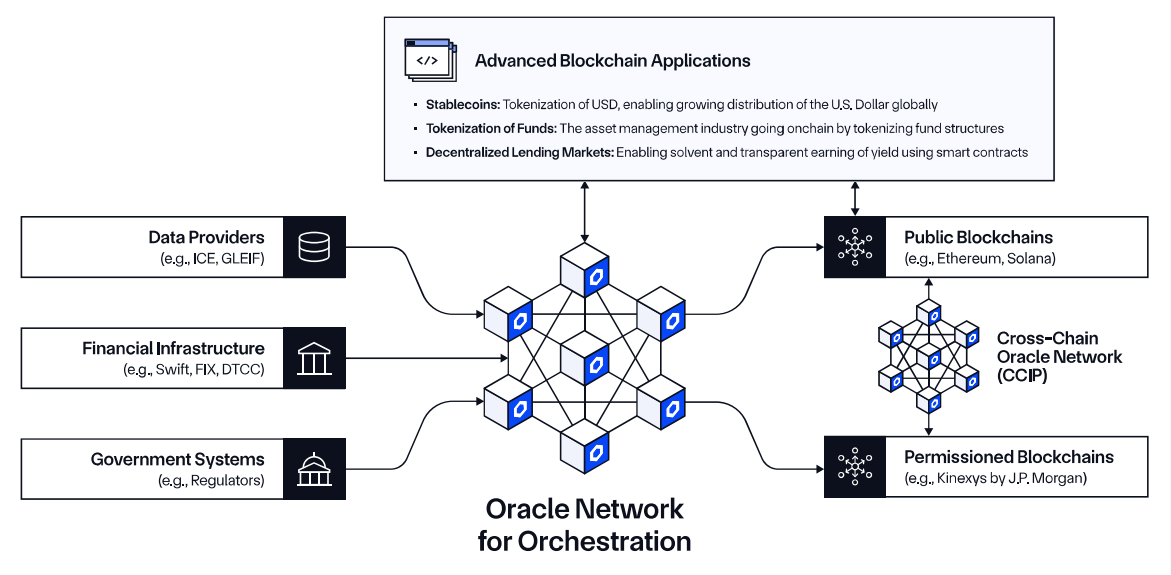
22 Graphic prepared by Consensys.

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.

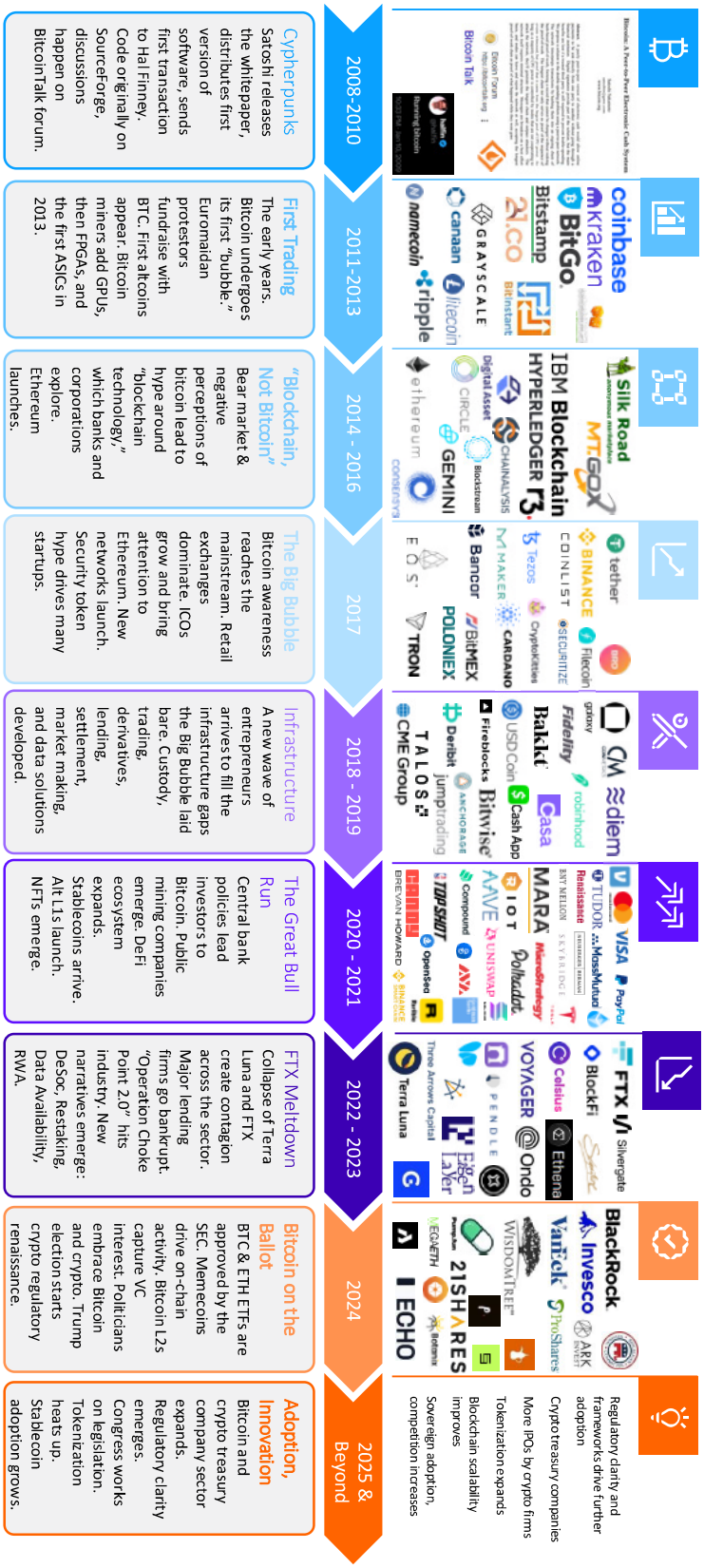
24 Press Release, Citigroup Inc., Citi Develops New Digital Asset Capabilities for Institutional Clients (Sept. 18, 2023), https://www.citigroup.com/global/news/press-release/2023/citi-develops-new-digital-asset-capabilities-for-institutional-clients; *see Franklin OnChain U.S. Government Money Fund,* 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 Blockchains*, 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).

Phases of Cryptocurrency and Digital Asset Market Adoption[28]



28 Graphic prepared by Galaxy.

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.

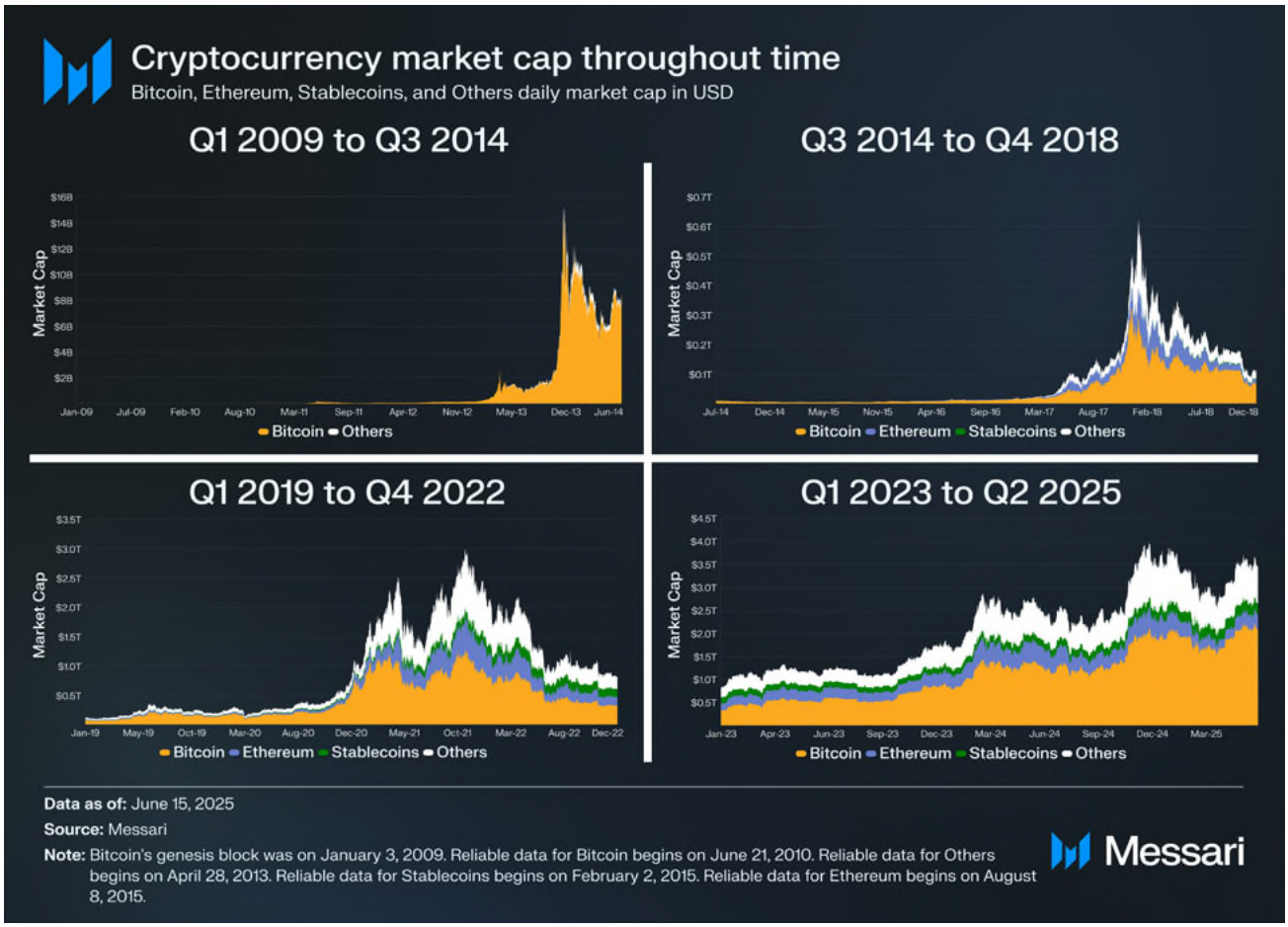
30 *See generally Why Are There So Many Cryptocurrencies and Why Do We Need Them*, Coinbase, https://www.coinbase.com/learn/crypto-basics/why-are-there-so-many-cryptocurrencies-and-why-do-we-need-them (last visited July 13, 2025).

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]

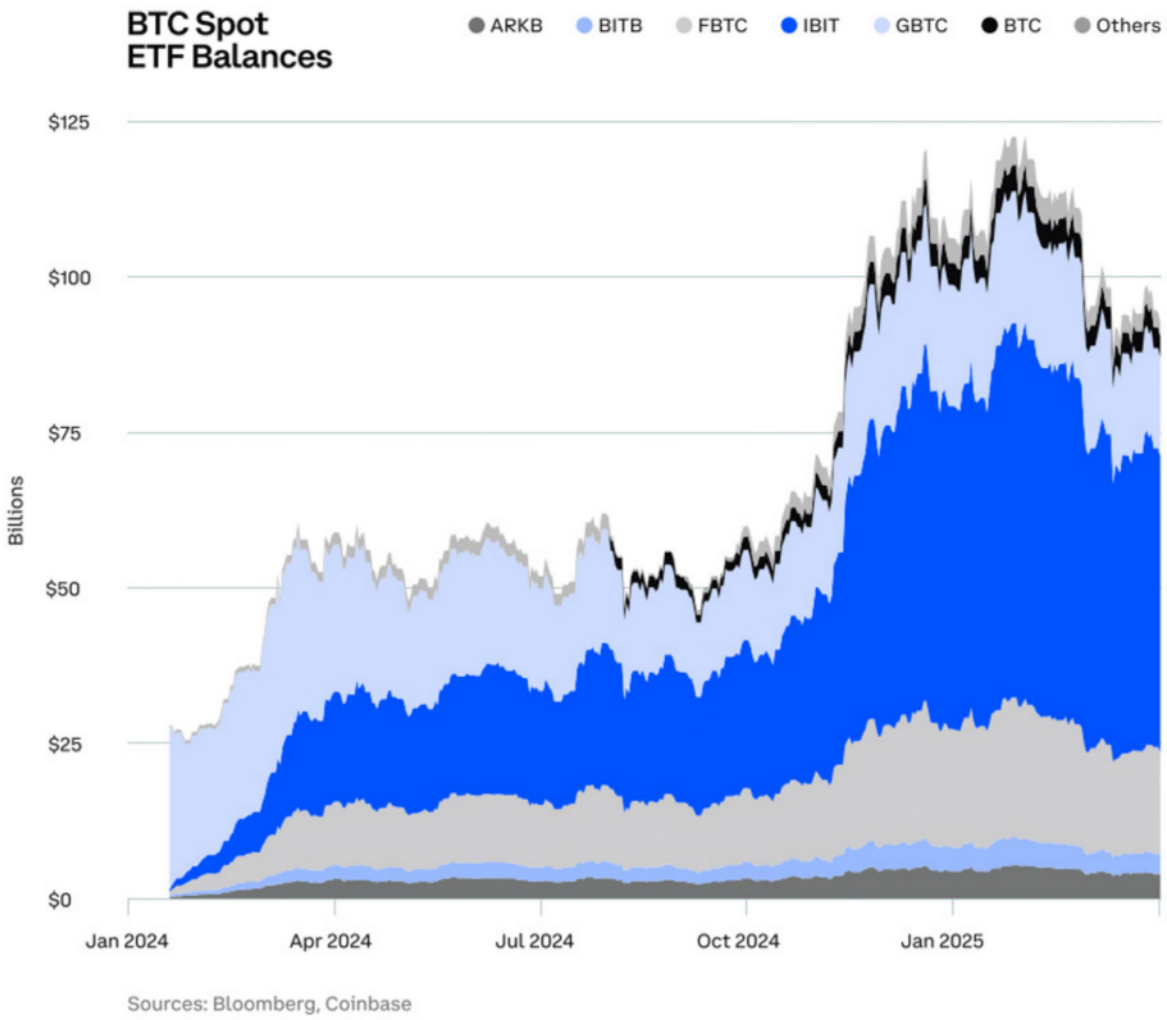
33 Graphic prepared by Messari.

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]

Participant	Description
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).

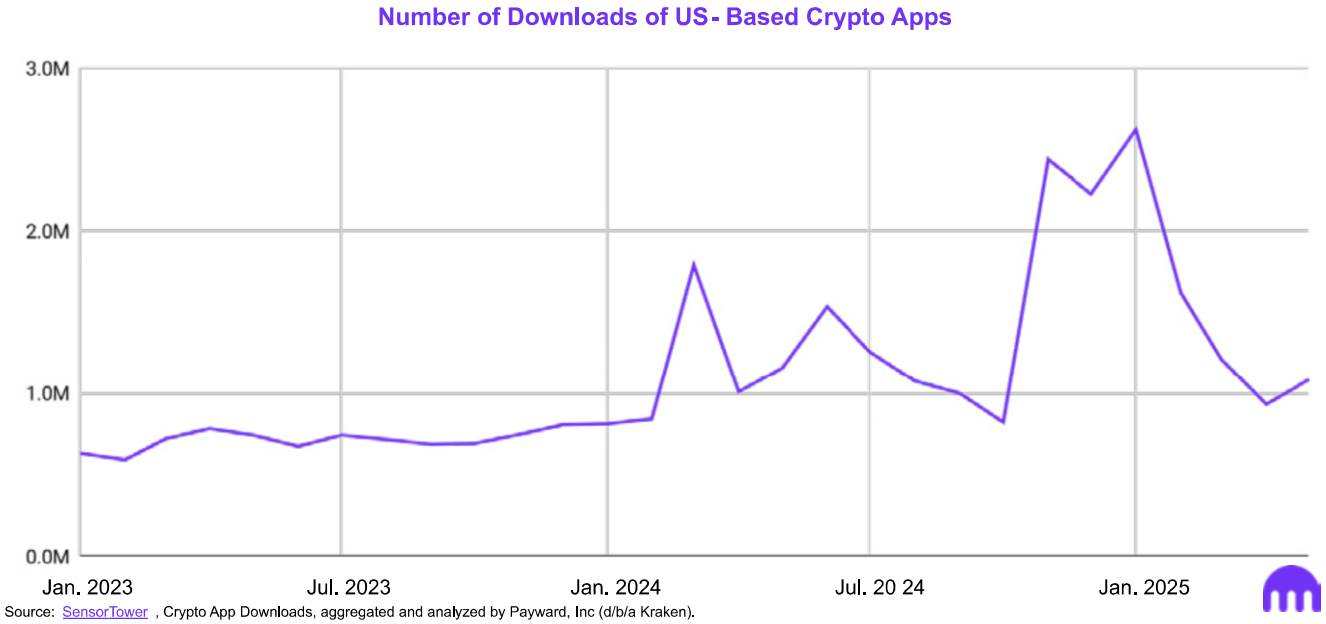
42 *See Chapter II, Mining and Staking* for a further discussion of actors supporting the operation of a blockchain's network.

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]



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.

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 of the Currency and Foreign Transactions Reporting Act, Pub. L. No. 91-508, its amendments, and the other statutes relating to the subject matter of that Act. These statutes are codified at 12 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).

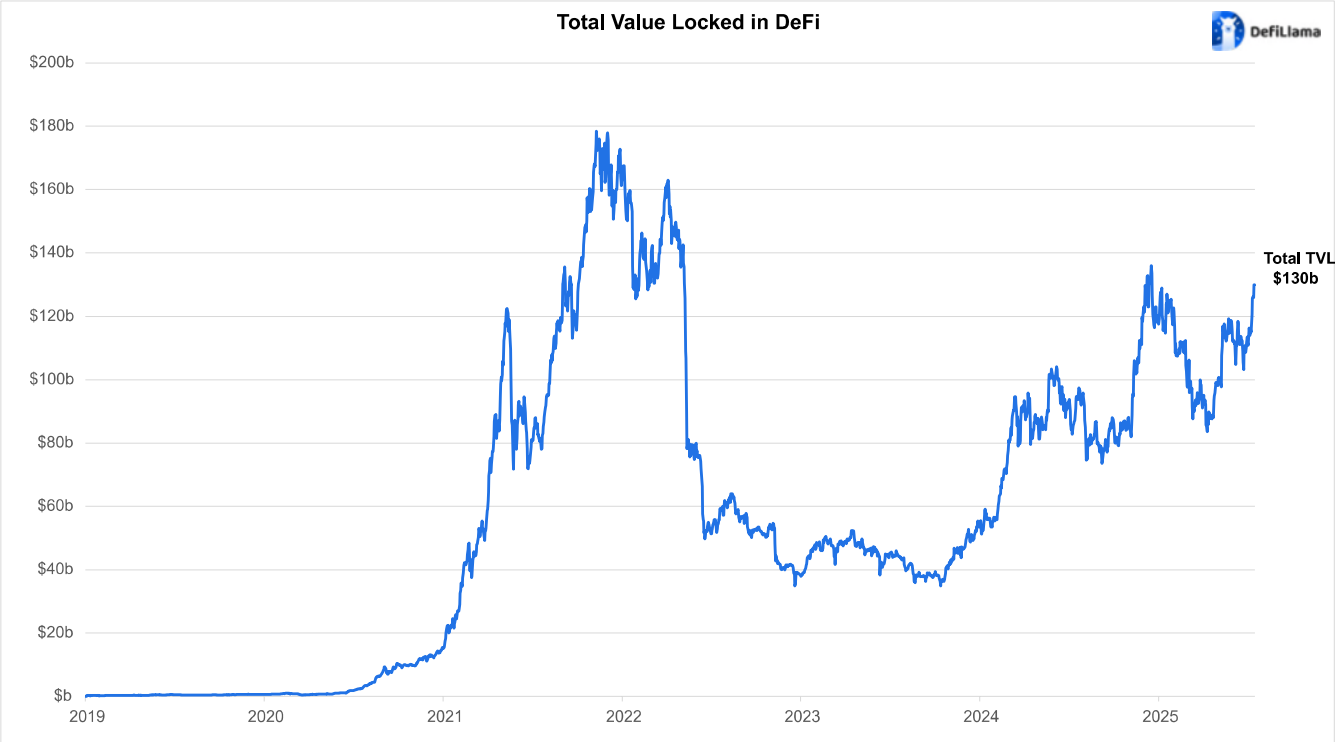
51 *See generally* 31 C.F.R. § 1022 (2024).

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.

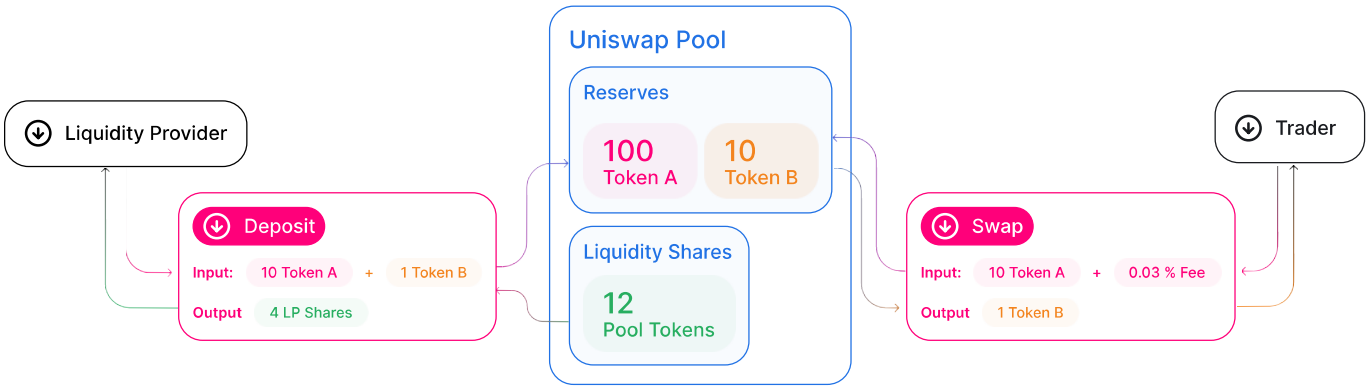
Like their centralized counterparts, DEXs offer users the ability to trade digital assets. In the absence of a central intermediary, DEXs typically rely on liquidity pools[61] and automated market-making[62] to provide trading services. DEXs tend to have lower transaction costs, greater transparency, 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 (@oxlchigo), *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 asset tokens that are native to a particular blockchain in a node to assist in the validation of transactions. Rather than spending compute resources in a race to produce a valid block, nodes proffer their own tokens, subjecting them to "slashing" or forfeiture if they 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 about regulatory 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-Service Program and Pay $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

Entity Type	Function
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 of the NFA. These SROs generally aim to establish and enforce standards, guidelines, and best practices that promote integrity, transparency, and consumer protection amongst their regulated 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 of federal securities laws, they provided non-accredited investors with the ability to obtain tokens at issuance.

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. *See 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.

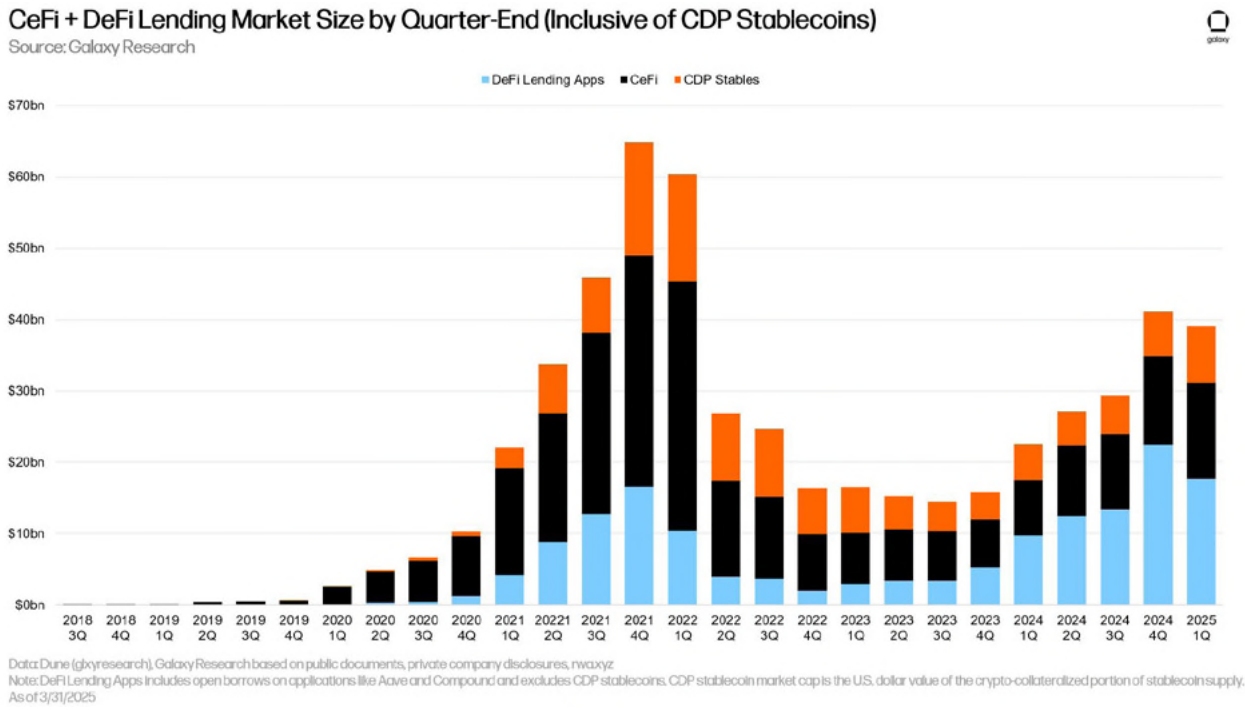
112 15 U.S.C. § 78q-1.

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 2025*, Galaxy (June 4, 2025), https://www.galaxy.com/insights/research/the-state-of-crypto-leverage-q1-2025.

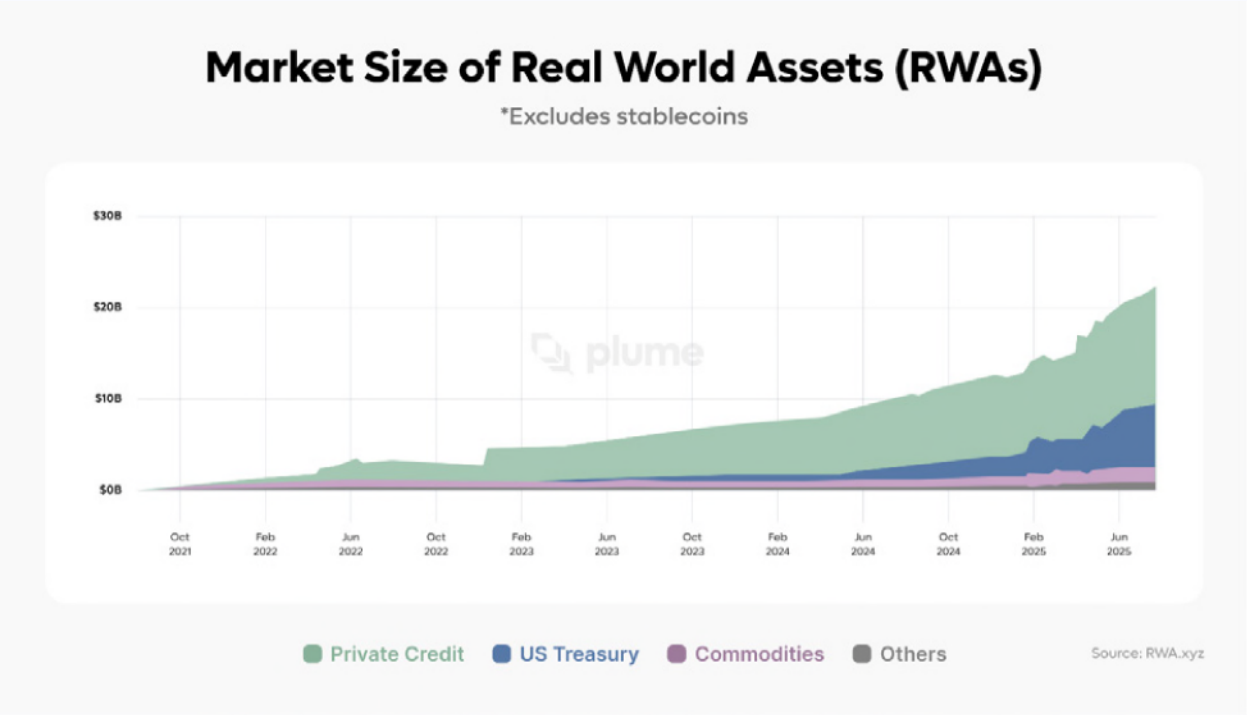
118 *See Blockchain Use Cases*, Consensys, https://consensys.io/blockchain-use-cases (last visited July 13, 2025); *The State of Crypto: The Future of Money Is Here Report*, Coinbase (Jun. 10, 2025), https://www.coinbase.com/blog/the-state-of-crypto-the-future-of-money-is-here.

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]



Similar to 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.

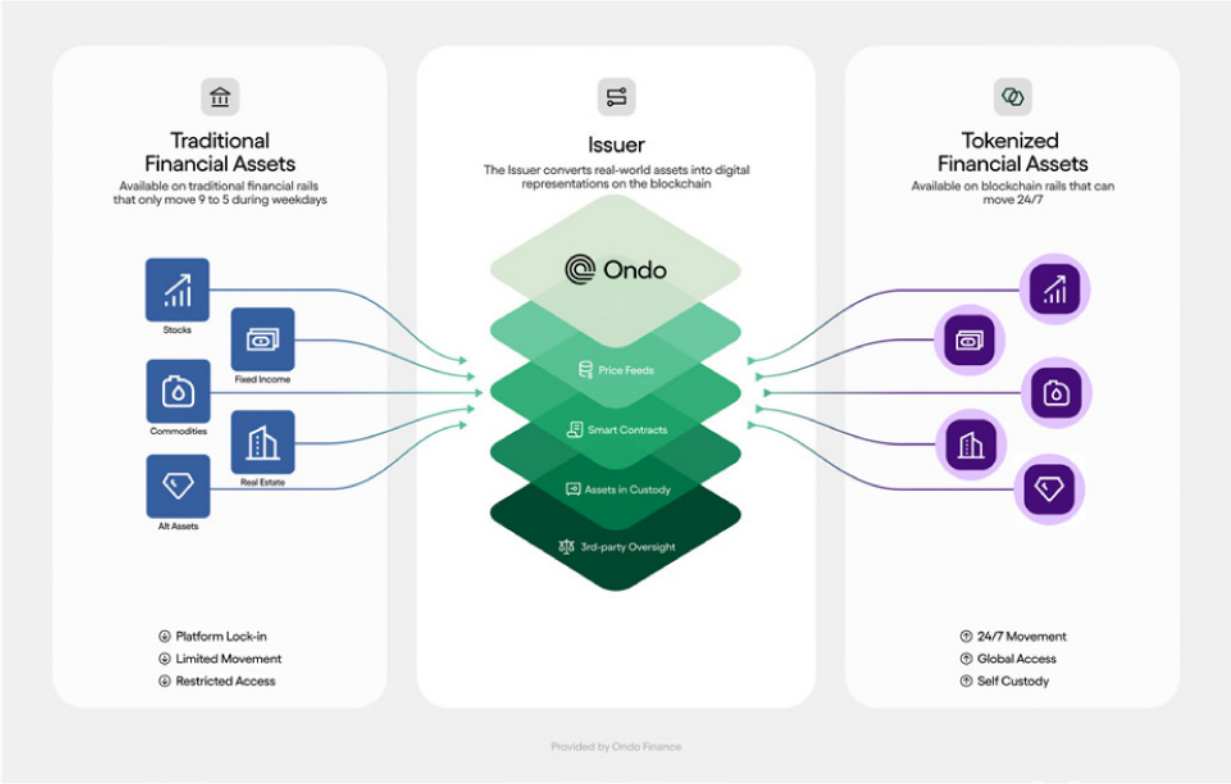
123 *See e.g.*, Sandy Kaul, *Tokenized Money Market Funds: The Bridge to a New Financial Infrastructure*, Franklin Templeton (Jun. 9, 2025), https://www.franklintempleton.co.uk/articles/2025/disruption/tokenized-money-market-funds-the-bridge-to-a-new-financial-infrastructure.

124 For a discussion of the benefits of atomic settlement in 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, but those processes can be resource intensive and prohibitively complex for smaller companies. NIST is an active participant in 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 control these 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, but releases 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 of the private key can fraudulently transfer and steal the 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.

SEC Actions	CFTC Actions
▪ 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) benefit from 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 subject to requirements under the Bank Secrecy Act, including anti-money laundering (AML) program requirements.[161] As a result, broker-dealers and mutual funds, among other registered entities, are required to implement reasonably-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) of the Exchange Act defines a "broker" as "any person engaged in the business of effecting transactions in securities for the 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 ether futures 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 subject to surveillance, reporting, and position limit rules 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 spot retail commodity transactions on digital assets pursuant to CEA section 2(c)(2)(D).
- Provide guidance as to how digital assets may be considered commodities under Section 1a(9) of the 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 or front ends can or should be required to comply with institutional obligations under the Bank Secrecy Act (BSA), either as money services businesses (MSBs), broker-dealers, FCMs, or some other category of "financial institution" under the 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 of the 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 adapt traditional procedures to address digital asset tokens. 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

The Working 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 asset frameworks, 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 payment instrument, limiting their circulation, their stability, or their ability to circulate without discount. Regulatory fragmentation can also lead to market fragmentation, and to reduced or trapped liquidity within specific stablecoin arrangements; this, in turn, can limit market depth in ways that can affect the 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 respect to 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.

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/000000000019d6689c085ae165831e934ff763ae46a2a6c172b3f1b60a8ce26f. *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 by Banking Organizations (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 asset industry 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 about risk, banks were initially slow to engage with digital assets. However, interest in digital asset-related product lines 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' interest in pursuing or increasing engagement with digital assets. Though banking agencies have steadily removed many of the previous regulatory impediments, certain areas of regulatory 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 appear to be focusing on the financial activities they view as most reliant 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 for lending 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 of the Biden Administration's Operation Choke Point 2.0 efforts to shut down interest from 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 Act to "set out a rebuttable presumption that it will exercise its discretion under that provision to limit state member banks to engaging as principal in only those activities that are permissible for national banks—in each case, subject to the terms, conditions, and limitations placed on national banks with respect to the activity—unless those activities are permissible for state banks by federal statute or under part 362 of the 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 other things, act as finder in 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 market in 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 at the 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 at the 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 engagement in 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 asset related activities without receiving 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 for risk management related 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.

federal safety nets under which a bank is supervised. A bank charter is essential for firms looking to provide a full suite of banking products and services as it grants certain needed legal authorities while often allowing the opportunity to apply for FDIC deposit insurance (or requiring the application) and obtain Reserve Bank payment services.

Obtaining a bank charter and FDIC insurance is a detailed, rigorous process designed to ensure that the financial institution applying will be financially sound, well-capitalized and well-managed, and capable of operating safely and in compliance with applicable banking rules and regulations.[278] Federal and state agencies generally use the Interagency Charter and Federal Deposit Insurance Application to collect information for and evaluate a de novo charter (a charter for a newly formed bank) and deposit insurance application, where applicable. While there are some differences in what is required and evaluated across different bank charter types, the interagency application gives a general overview of what banks are required to consider.[279] Some firms considering a bank charter have expressed frustration with a lack of clarity on timing for completing the process and transparency on the application process.[280]

Master Accounts

A Reserve Bank master account is a deposit account maintained by a bank or other type of depository institution at a regional Reserve Bank and provides a gateway to the Federal Reserve's balance sheet, which is used to promote financial stability and conduct monetary policy. A master account "is both a record of financial transactions that reflects the financial rights and obligations of an account holder and of the Reserve Bank with respect to each other, and the place where opening and closing balances are determined."[281] The Federal Reserve Act authorizes the FRS to hold deposits—which, as noted, are held in master accounts—for depository institutions, FRS member banks, and certain U.S. branches and U.S. agencies of foreign banks.[282] Depository institutions and other eligible entities use deposits held in a master account at the Federal Reserve for the settlement of interbank payments.

Institutions seeking a master account must request access from their regional Reserve Bank. The Reserve Banks utilize guidelines approved by the FRB in 2022 when evaluating requests for a master account.[283] Some firms that may be eligible for a master account have expressed frustration with a lack of clarity on timing for completing the process though the FRB is providing transparency on process outcomes.

278 *See* 12 C.F.R. § 5.20 (2025); OCC, Comptroller's Licensing Manual: Charters (Dec. 2021), https://www.occ.treas.gov/publications-and-resources/publications/comptrollers-licensing-manual/files/charters.pdf; 12 C.F.R. pt. 303 (2025); FDIC, Applying for Deposit Insurance: A Handbook for Organizers of De Novo Institutions (Dec. 2019), https://www.fdic.gov/regulations/applications/depositinsurance/handbook.pdf; FDIC, Deposit Insurance Applications: Procedures Manual Supplement - Applications from Non-Bank and Non-Community Bank Applicants (Dec. 2019), https://www.fdic.gov/regulations/applications/depositinsurance/procmanual-supplement.pdf.

279 *See* Andrew P. Scott, An Analysis of Bank Charters and Selected Policy Issues, CRS R47014 (2022) ("The application's basic structure covers the following areas: overview of institution's business model, activities, public and private offerings, and the articles of association or incorporation and bylaws; description of the management, including directors, executives, officers, board members, conflicts of interest, and stock benefit plans; details of the institution's capital plans, including capital to be raised, class and amount of stock to be issued, capital adequacy projections, and corporate tax status; description of how the institution meets the needs of the community, consistent with its business plan, and a separate plan to meet obligations pursuant to the [Community Reinvestment Act]; description of the premises and fixed assets, security plans to protect property, plans to establish branches, and identification of the main office; records of the information systems used, including a description of the physical and logical components of security systems used; other information, such as functions to be outsourced, fidelity coverage, a plan to comply with the Bank Secrecy Act, and the organization's planned expenses.").

280 The OCC's Licensing Manual states that the OCC seeks to make a decision within 120 days after receipt of a complete application via a standard submission. OCC, *supra* note 278, at 36.

281 FRB, Reserve Maintenance Manual 5 (Nov. 2019), https://www.federalreserve.gov/monetarypolicy/files/reserve-maintenance-manual.pdf.

282 12 U.S.C. §§ 342, 347d. Section 19(b)(1)(A) of the Federal Reserve Act defines depository institution for purposes of the Federal Reserve Banks' authority to maintain deposits. 12 U.S.C. § 461(b)(1)(A). The Reserve Banks are also permitted to maintain accounts for other entities, including foreign banks, foreign states or as fiscal agent of the United States. 12 U.S.C. §§ 358 and 391.

283 Guidelines for Evaluating Account and Services Requests, 87 Fed. Reg. 51099 (Aug. 19, 2022).

Recommendations

- **Provide clarity and transparency regarding the process for eligible institutions to obtain a bank charter or a Reserve Bank master account.**
  - The relevant Banking Agencies should clarify and define in regulation the expected timelines for decision-making on completed applications for charter licensing (including federal deposit insurance where applicable) and requesting a Reserve Bank master account.
  - If regulatory timelines are not met for a given application, the application should be deemed approved absent extraordinary circumstances.
  - The Banking Agencies should also confirm that otherwise eligible entities are not prohibited from obtaining bank charters, obtaining federal deposit insurance, or receiving Reserve Bank master accounts or services solely because they engage in digital asset-related activities.
  - Finally, the Banking Agencies should provide additional transparency, as appropriate, on the number of, and average time to review, complete applications, including new charter applications, federal deposit insurance applications, and Reserve Bank master account applications, on both an aggregated and annual basis.

Federal Credit Unions

Some credit unions have engaged in the digital asset ecosystem primarily as service providers to digital asset market participants or as intermediaries facilitating member access to these markets.

- **Traditional (Core) Financial Services:** Similar to banks, some credit unions offer core financial services to digital asset-related businesses, including deposit accounts, payment services, and settlement capabilities. NCUA share insurance only covers member shares (akin to bank deposits) at most credit unions. As a result, digital asset firms frequently partner with credit unions designated as low-income (LICUs), as share insurance covers both member and non-member shares at these institutions.
- **Custody and Member Access Services:** A small but growing number of credit unions have explored partnerships to facilitate digital asset custody. Several credit unions facilitate digital asset exchange services (buy, sell, and hold cryptocurrency assets) through third-party platforms, with information relating to digital asset holdings integrated into the credit union's digital banking experience.
- **Tokenization and DLT Use:** Select credit unions and Credit Union Service Organizations (CUSOs) are exploring the use of DLT to improve internal operations, streamline settlement, and participate in stablecoin operations (issuing payment stablecoins through a CUSO and serving as a depository institution for fiat currency reserves). A small number of credit unions are exploring but have not yet implemented tokenization of financial assets or member shares.
- **Digital Asset Lending:** A limited number of credit unions have expressed interest in originating loans secured by certain digital assets.

Current Regulatory Framework

- **Legal Permissibility:** The NCUA has issued guidance that affirms that credit unions are not prohibited from using DLT if they comply with applicable laws and regulations.[284]

284 NCUA, 22-CU-07, Federally Insured Credit Union Use of Distributed Ledger Technologies (May 2022), https://ncua.gov/regulation-supervision/letters-credit-unions-other-guidance/federally-insured-credit-union-use-distributed-ledger-technologies.

  - Federally chartered and insured credit unions are subject to field-of-membership requirements and statutory limits on permissible activities, raising unique questions related to share insurance coverage. In 2024, the NCUA updated the Share Insurance FAQs to clarify that share insurance does not cover digital assets or cryptocurrencies.[285]
  - The Federal Credit Union Act (FCUA) only provides limited authority for federal credit unions to provide custody services. The FCUA does not provide explicit authority for federal credit unions to provide custody or safekeeping services, and these custody services are provided through third parties. Additionally, state-chartered and privately insured credit unions may be permitted to provide custody services if permitted by state law.

- **Supervision:** Credit unions would like additional clarity on risk-management and compliance expectations.
- **Capital and Other Applicable Regulatory Treatment:** The NCUA Final Rules on Risk Based Capital (RBC) and Complex Credit Union Leverage Ratio (CCULR) do not specifically address risk weights for digital assets. Therefore, if credit unions hold these assets, they would fall into the catch-all category, which is 100%.
  - Only complex credit unions with total assets of $500 million or more are subject to risk-based capital requirements under NCUA's RBC and CCULR frameworks.

Access to Providing Banking Services

CUSOs play a key role in expanding access to digital asset services for credit unions and their members. These entities have piloted offerings in custody, payments, and tokenization. However, many CUSOs seek clarity around what services they can provide on behalf of credit unions and what level of NCUA oversight or registration is required for such activities.

Capital and Other Applicable Regulatory Treatment

The U.S. risk-based capital framework does not contain any provisions specific to cryptoasset[286] exposures. Under the current U.S. capital framework, the risk weight assigned to a novel exposure, such as an exposure to a cryptoasset depends on several factors, including whether the asset is a security or a commodity. The U.S. Banking Agencies and Treasury should advocate for modernization of the international Basel Committee on Banking Supervision (BCBS) standards to incorporate new data on digital asset market performance and risk and recent DLT technological innovations.

BCBS Cryptoasset Exposures Capital and Liquidity Standards

In December 2022, the BCBS published its standard on the prudential treatment of cryptoasset exposures.[287] The standard was later amended in July 2024.[288] The BCBS framework divides cryptoassets into two groups. Group 1 assets, which are cryptoassets that reference or are otherwise backed by other traditional assets or exposures and meet several specified conditions, are subject to capital requirements based on the risk weights

285 *Frequently Asked Questions About Share Insurance: Digital Assets and Cryptocurrencies*, NCUA, https://ncua.gov/consumers/share-insurance-coverage/frequently-asked-questions-about-share-insurance (last modified May 28, 2024).

286 This section (*Capital and Other Applicable Regulatory Treatment*) uses the term "cryptoasset" instead of "digital asset" to match the term used by BCBS. However, the terms are intended by this report to be interchangeable. Note, however, that BCBS understands the terms to differ slightly in meaning. BCBS, *supra* note 204, at 5 ("Cryptoassets are defined as private digital assets that depend on cryptography and distributed ledger technologies (DLT) or similar technologies. Digital assets are a digital representation of value, which can be used for payment or investment purposes or to access a good or service.").

287 BCBS, *supra* note 204.

288 BCBS, *supra* note 205.

of the underlying exposures.[289] Group 1 assets are further divided into Groups 1a and 1b.[290] Group 1a includes tokenized traditional assets, and Group 1b includes stablecoins that meet certain classification conditions.[291] Group 2 comprises cryptoassets that fail to meet at least one Group 1 classification condition.[292] Within Group 2, cryptoassets that meet hedge recognition criteria would fall under Group 2a, and those that do not would fall under Group 2b.[293]

Generally, cryptoassets that are grouped into Group 1a are subject to the existing capital rules for traditional assets.[294] For Group 1b assets, banks must analyze all the risks that could cause a loss (e.g., credit risk from reference assets, risk of default of the redeemer, etc.) and capitalize for those risks individually using the credit risk standards. In addition to the capital requirement, there is a potential add-on for infrastructure risk for Group 1 assets.[295] The standard sets the initial add-on at 0, but national authorities can initiate or increase the add-on based on observed weakness in the infrastructure of specific cryptoassets.[296]

Capital treatment for Group 2a involves adapted market risk rules and a 100% capital charge on the exposure's net position.[297] Group 2b cryptoassets are those that do not meet hedging criteria and thus are not permitted to recognize hedging and are subject to a 1250% risk weight.[298] Examples of Group 2 cryptoassets include bitcoin and ether,[299] which together comprise over 70% of the total value of the digital asset market.[300]

289 BCBS, *supra* note 204, at 1.

290 At a high level, in order to be classified as Groups 1a or Group 1b, a cryptoasset must meet the following classification conditions: (i) the cryptoasset must either be a tokenized traditional asset or have a stabilization mechanism that is considered effective at all times in linking its value to a traditional asset or a pool of traditional reference assets; (ii) all rights, obligations and interests arising from the cryptoasset arrangement are clearly defined and legally enforceable in all the jurisdictions where the asset is issued and redeemed, and the applicable legal framework ensures settlement finality; (iii) the functions of the cryptoasset and the network on which it operates, including the distributed ledger or similar technology on which it is based, are designed and operated to sufficiently mitigate and manage any material risks; and (iv) entities that execute redemptions, transfers, storage, or settlement finality of the cryptoasset, or manage or invest reserve assets, must be regulated and supervised, or subject to appropriate risk management standards, and have in place and disclose a comprehensive governance framework. *Id.* at 1.

291 *Id.* at 6, 9-10.

292 *Id.* at 1.

293 There are three hedge recognition criteria for Group 2a cryptoassets. First, the exposure needs to be either (i) a direct holding of a spot Group 2 cryptoasset where there is a derivative or ETF that is traded on a regulated exchange and solely references the cryptoasset; (ii) a derivative or ETF/exchange-traded note (ETN) that references a Group 2 asset, and that derivative has been explicitly approved by market regulators or a qualifying central counterparty; (iii) a derivative, ETF, or ETN that references a derivative meeting the previous requirement; or (iv) a derivative, ETF, or ETN, that references a related reference rate that is published by a regulated exchange. Second, the exposure or reference exposure must have at least a $10 billion average market cap over the previous year and the 10% trimmed mean of daily trading volume with major fiat currencies must be at least $50 million over the prior year. Third, sufficient data availability is required. Specifically, there need to at least 100 "real" price observations over the previous year and there must be sufficient data on trading volumes and market capitalization. *Id.* at 1, 17-18.

294 *Id.* at 12.

295 *Id.* at 13.

296 *Id.* at 17.

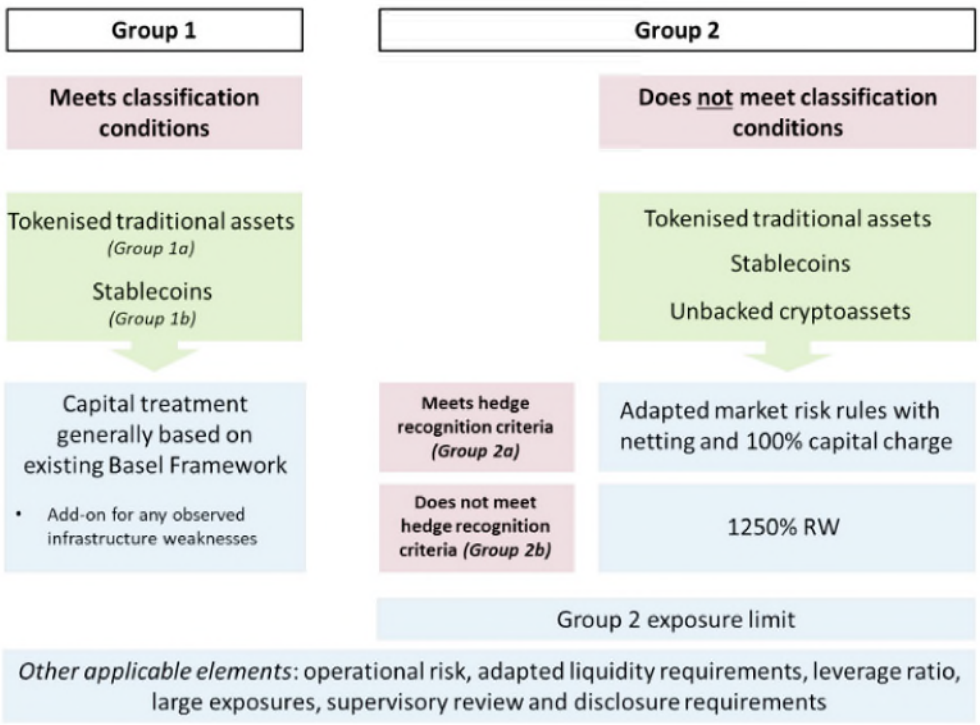
297 *Id.* at 17-19.

298 *Id.* at 17, 21.

299 Global Financial Markets Association, et al., Re: Comments in Response to the Second Consultation on the Prudential Treatment of Cryptoasset Exposures (Sept. 23, 2022), https://www.icmagroup.org/assets/Joint-TA-response-to-BCBS-2nd-consultation-crypto-assets-30092022.pdf.

300 *See* CoinMarketCap.com, https://coinmarketcap.com/ (last visited July 13, 2025).

Categorizing Cryptoassets into Basel Group 1 or Group 2[301]



The BCBS framework also includes a limit for a bank's Group 2 exposures.[302] Both direct (cash and derivatives) and indirect holdings (e.g., those via investment funds, exchange-traded funds (ETFs)/exchange-traded notes (ETNs), or any legal arrangements designed to provide exposure to cryptoassets) should not amount to more than 1% of Tier 1 capital and functionally cannot exceed 2%.[303] Any breach that does occur must be communicated to the supervisor, and until compliance with the 1% limit is restored, a bank's exposures that exceed the threshold are subject to the capital requirements that apply to Group 2b cryptoasset exposures.[304] If the threshold of 2% is actually exceeded, all Group 2 cryptoasset exposures (not just those in excess of 1%) will be subject to the capital requirements that apply to Group 2b cryptoasset exposures.[305]

Cryptoassets are included in the BCBS leverage ratio exposure measure according to their value for financial reporting purposes, based on applicable accounting treatment for exposures that have similar characteristics. For the cases where the cryptoasset exposure is an off-balance sheet item, the relevant credit conversion factor set out in the leverage ratio framework will apply in calculating the exposure measure.[306]

Under the BCBS liquidity standards,[307] Group 1a cryptoasset and crypto-liability exposures are generally treated consistent with exposures involving their equivalent non-tokenized traditional assets and liabilities,

301 BCBS, *supra* note 204, at 6.

302 *Id.* at 28.

303 *Id.*

304 To reduce cliff effects, which can create a significant increase in regulatory capital required once a bank crosses a given threshold, if a bank breaches the 1% limit, the Group 2b 1250% risk weight would apply to only the amount which exceeds the limit and not to all Group 2 exposures, but if the 2% limit is breached the whole of Group 2 exposures would be subject to the 1250% risk weight. *Id.* at 32.

305 *Id.* at 28.

306 *Id.* at 27.

307 Such standards are the liquidity coverage ratio and net stable funding ratio.

including qualification as high-quality liquid assets (HQLA).[308] Group 1b and Group 2 cryptoassets do not qualify as HQLA,[309] and corresponding asset and liability exposures are treated with inflow and outflow rates and required stable funding and available stable funding factors tied to the maturity of the coin (i.e., 30 days, 6 months, 1 year) and the underlying collateral (HQLA vs non-HQLA).[310]

The second consultation on the BCBS standard (published before the standards were finalized in December 2022) states that "as currently specified, it is highly unlikely that any cryptoassets based on permissionless blockchains will be able to meet the classification conditions to be included in Group 1."[311] However, in the final standard, the Committee notes that the BCBS will continue to reflect on whether the risks posed by cryptoassets that use permissionless blockchains can be sufficiently mitigated to allow for their inclusion in Group 1 and, if so, what adjustments to the classification conditions would be needed.[312]

The BCBS does not possess any formal supranational authority, and its decisions do not have legal force. In principle, the "standards" set by the BCBS are determined by consensus of BCBS members.[313] It is important for the United States to lead in such international forums to ensure transparency of any such consensus decision making.

Recommendations

- **The Banking Agencies should clarify the circumstances, using risk-based guidelines, under which tokenized assets and tokenized asset collateral would be subject to the same capital and liquidity treatment as the underlying asset or collateral.**
- **The United States should adopt capital requirements for bank digital asset activities that accurately reflect the risk of the asset or activity. Additionally, the United States should advocate that the BCBS revisit the cryptoasset standards to ensure similar treatment to U.S. capital requirements.**

In adopting capital requirements for bank digital asset activities, the following actions should be taken to evaluate and improve the BCBS cryptoasset standards:

- **Simplification of the cryptoasset grouping.**
  - BCBS's four groups of cryptoassets should be simplified. Applying a separate classification to traditional assets due to the use a specific technology does not adhere to the principle of technology-neutrality. Furthermore, the treatment of tokenized traditional assets as cryptoassets is misleading and may create unintended negative consequences.[314] Additionally, the BCBS distinction between Group 2a and Group 2b cryptoassets does not create a clear enough distinction between cryptoassets widely used for payment and investment purposes and other cryptoassets, such as memecoins.
  - The U.S. prudential cryptoasset framework should: (i) clarify when tokenized traditional assets are equivalent to traditional assets and are subject to the same capital and liquidity requirements as traditional assets; (ii) work to align the BCBS definition of stablecoins eligible for Group 1b treatment with requirements set forth in GENIUS; and (iii) simplify the classification of Group 2 cryptoassets and address the treatment of cryptoassets outside of Group 2.

308 Group 1a tokenized claims of a bank not secured by an underlying pool of assets would be treated under BCBS liquidity standards as unsecured funding, with the outflow rates and ASF factors linked to the type of customer (retail, wholesale, financial) and the term (30 days, 6 months, 1 year), and cannot be treated with as stable retail deposit or certain preferential operational deposits. *Id.* at 24.

309 *Id.*

310 *Id.* at 26-27.

311 BCBS, Second Consultation on the Prudential Treatment of Cryptoasset Exposures 4 (June 2022), https://www.bis.org/bcbs/publ/d533.pdf.

312 BCBS, *supra* note 204, at 4.

313 BCBS, Basel Committee Charter § 8.4 (updated June 5, 2018), https://www.bis.org/bcbs/charter.htm.

314 For example, treating tokenized traditional assets differently from traditional assets may hinder their eligible collateral status.

- **Use of permissionless blockchain for all groups of cryptoassets.**
  - Under the BCBS standards, cryptoassets relying on permissionless blockchains pose risks that may prevent them from being included in Group 1. However, experimentation and testing with permissionless blockchains by regulated financial institutions suggests that technical solutions to mitigate the risks identified by the BCBS are being actively developed and implemented.[315] The BCBS also raises concerns with the probabilistic settlement of permissionless blockchains.[316] However, over the last several years, market participants have been developing industry standards for determining when a settlement has completed on probabilistic blockchains.
  - The United States should consider incorporating those standards to inform the prudential treatment of those characteristics of distributed ledger technology.
- **Review the calibration of capital requirements for credit risk, market risk, operational risk, and liquidity risk to incorporate empirical evidence of recent changes in cryptoasset performance and risk.**
  - Changes in the grouping of cryptoassets may not fully modernize the BCBS cryptoasset prudential standards. The United States should also revisit the calibration of the prudential standards to consider incorporating recent innovations and changes in the cryptoasset market since the BCBS standards were first published in 2022.
  - The Banking Agencies should undertake a comprehensive data analysis on the performance and risk of cryptoassets informed by issuing a request for information from the public, inclusive of representatives from cryptoasset data vendors, distributed ledger infrastructure providers, banking organizations of all sizes, and industry associations. The analysis would assist the Banking Agencies in determining the appropriate calibration for cryptoasset capital and liquidity standards.

Insurance and Digital Assets

Insurance is important for U.S. consumers, the economy, and the financial system.

Digital assets can be a significant part of the net worth of an individual or business. The cost and availability of adequate digital asset insurance affects the growth and stability of the digital asset market.

Insurability

Insurable events have four characteristics that are relevant to the analysis of the insurability of digital assets. First, insurable events must be "pure risks," meaning they cannot result in gain, only loss. Thus, events like a decline in a business's revenues or the market value of an asset are generally not insurable. Second, they must be defined, reasonably uncorrelated, measurable, and limited. An insurer must be able to measure a loss objectively and limit that loss contractually. Third, insurable events must be unpredictable individually, but predictable in the aggregate. Finally, insurable events must be random and unintentional from the standpoint of an insured.[317] These principles inform what events can and cannot be covered, as discussed further below.

315 For example, depending on the programmability of the cryptoasset, the cryptoasset can be permissioned by smart contracts (e.g., an ERC1400 token on Ethereum). Such standards allow the role of a "controller" (i.e., an actor that can control access, freeze, reverse, or destroy cryptoassets or block transactions), enabling compliance with know-your-customer, anti-money laundering, and countering the financing of terrorism checks.

316 Specifically, it noted that in many permissionless distributed ledger technologies, settlement remains probabilistic, meaning the probability that a transaction could be revoked converges to, but never reaches, zero with the passage of time. This could create settlement risk in permissionless blockchains.

317 *See* Judy Feldman Anderson & Robert L. Brown, Risk and Insurance, Education and Examination Committee of the Society of Actuaries 5-6 (2005), https://www.soa.org/globalassets/assets/files/edu/P-21-05.pdf.

Coverages

There are broadly two types of insurance relevant to the digital asset market. The first is insurance provided for individuals, or "personal lines."[318] The second is insurance provided for businesses and organizations, or "commercial lines."[319] The personal lines market for digital assets is currently limited. The lack of a robust personal lines market for digital assets may be caused by various factors, including regulatory uncertainty both domestically and globally, the lack of historical underwriting experience, potential volatility in certain types of digital assets, uncertainty regarding how courts will interpret insurance policy language, and questions regarding whether digital assets would be classified as currencies or personal property.[320] However, there is a small but growing commercial lines market. Treasury's Federal Insurance Office estimates that twenty insurers provide various types of commercial insurance for digital assets with limits up to $1 billion. Gross revenue has been estimated to be between $1.94 billion and $3.11 billion.[321] Large commercial insurance brokerages and both new and established insurance companies all participate in the digital asset insurance market.

The following types of insurance coverage for commercial entities, such as digital asset exchanges, custodians, asset managers, commercial mining operations, etc. are generally available, with generally broader coverage terms and limits for cold storage versus hot storage:

- Various forms of theft, such as embezzlement, fraud, malicious destruction of digital assets, kidnap, ransom, or extortion, etc. This type of coverage would indemnify, for example, a digital asset custodian if an employee destroyed a cold wallet.
- Damages incurred because of professional errors (referred to as errors and omissions coverage) or errors in software (known as cyber or tech errors and omissions coverage). For example, this type of coverage could indemnify a software company whose code inadvertently allowed for a malicious outside actor to steal digital assets from a hot wallet.
- Accidental loss or destruction of digital assets or keys. This insurance coverage would, for example, indemnify a digital asset manager for the loss of a cold storage wallet.
- Other standard coverages for any commercial entity, such as property, directors and officers, general liability, etc. Directors and officers insurance indemnifies the board of directors and senior officers of a company for certain damages awarded in the event of shareholder litigation. Property insurance would cover a warehouse and air conditioning system for a digital asset mining operation. General liability would indemnify a mining operation for damages accidentally sustained by a third party due to the negligence of the mining operation.

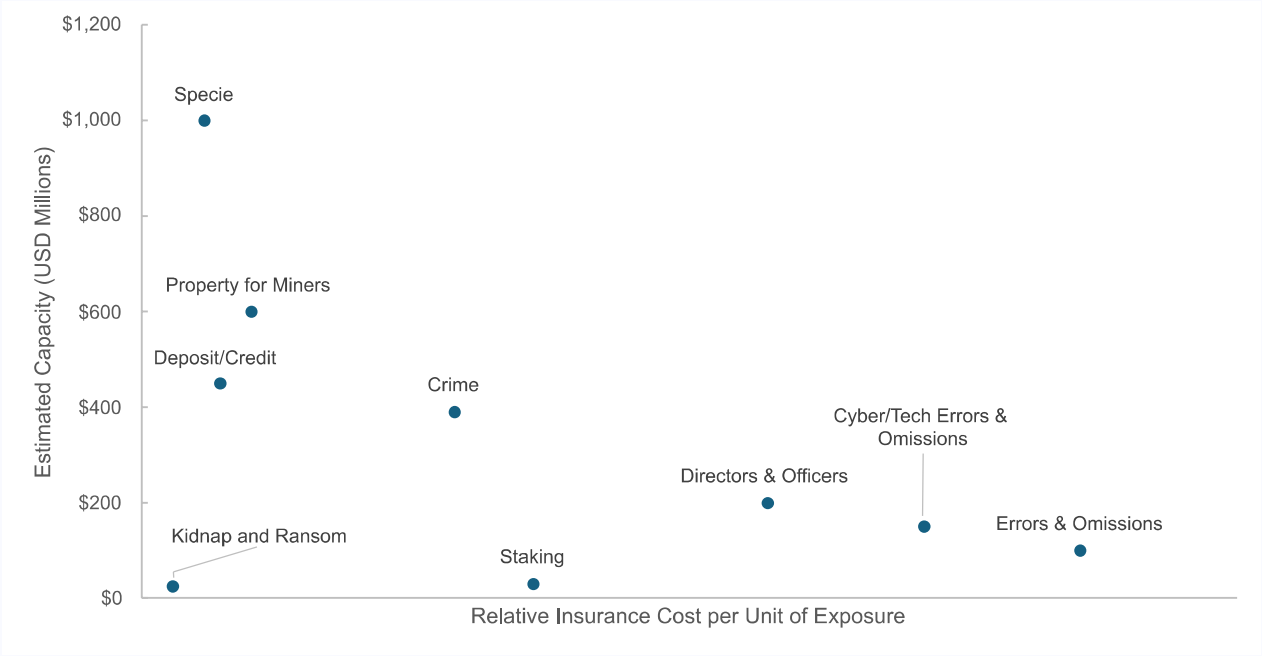
318 *Facts + Statistics: Commercial Lines*, Insurance Information Institute, https://www.iii.org/fact-statistic/facts-statistics-commercial-lines (last visited July 13, 2025).

319 *Id.*

320 Chantal M. Roberts, *Crypto Is a Popular Cybercrime Target, but Insurance Options Remain Limited*, Bankrate (May 5, 2025), https://www.bankrate.com/insurance/cryptocurrency-insurance-options-remain-limited/.

321 Joe Toppe, *How Insurance Plays a Role in Cryptocurrency Risks*, PropertyCasualty360 (Mar. 25, 2025 at 11:15 AM), https://www.propertycasualty360.com/2025/03/25/how-insurance-plays-a-role-in-cryptocurrency-risks.

Examples of Estimated Digital Asset Insurance Capacity and Relative Cost[322]



State Regulation of Insurance

The business of insurance in the United States is primarily regulated at the state level.[323] Insurance laws are enacted by state legislators and governors and are implemented and enforced by state regulators. Broadly speaking, state regulation is divided into prudential regulation (frequently referred to as "solvency" regulation) and marketplace regulation. Prudential regulation consists of oversight of an insurer's financial condition and its ability to satisfy policyholder claims. Marketplace regulation governs an insurer's business conduct, such as the pricing of premiums, advertising, minimum standards governing the terms of insurance policies, and licensing of insurance agents and brokers (producers), together with general issues of consumer protection and access to insurance.

Regulatory and Market Issues or Challenges

Some regulatory and market issues or challenges for digital asset insurance are:

- Existing federal regulations such as the CFTC's definition of a "swap" require that insurance products have a beneficiary with an insurable interest in the insured asset, limit payout to the insurable interest, and have the same beneficiary with an insurable interest throughout the duration of the insurance product. This definition is relevant because an insurance product cannot cover the loss of market value of a digital asset, such as a stablecoin. Any "insurance" policy marketed as covering a loss in market value of a digital asset would fall out of the insurance safe harbor of federal regulations.[324]
- As noted above, homeowners insurance policies generally do not cover, or highly restrict, digital assets.

322 Graphic based on information provided by Aon plc.

323 U.S. Department of the Treasury Federal Insurance Office, How to Modernize and Improve the System of Insurance Regulation in the United States 1 (2013).

324 Further Definition of "Swap," "Security-Based Swap," and "Security-Based Swap Agreement"; Mixed Swaps; Security-Based Swap Agreement Recordkeeping, 77 Fed. Reg. 48208 (Aug. 13, 2012).

- Insurers must match their forecasted liabilities to their assets. State prudential regulations require insurance companies to invest the vast majority of their assets in stable forms so that insurers can eventually pay claims. Insurers that take payment in digital assets but pay claims in fiat currency, or vice versa, take on volatility risk that may undermine their regulatory compliance.

Potential Policy Actions

There are various steps Treasury and state regulators could take to help improve regulatory certainty and develop a more robust market for digital asset insurance:

- Engage with the appropriate regulatory agencies to establish or amend legal definitions of securities, property, or currency so that insurance policies explicitly cover digital assets.
    - Treasury could also work with the insurance sector to create standardized terms, conditions, and policy language for digital assets.
- Engage with the National Association of Insurance Commissioners (NAIC) and state insurance regulators on potential revisions to state regulations relating to digital assets, including allowing insurers to invest in digital assets, as appropriate.
- Prioritize engagement between the public and private sector to help develop a robust insurance market for digital assets.

CHAPTER V

Stablecoins and Payments

Stablecoins and Payments

> With e-currency based on cryptographic proof, without the need to trust a third party middleman, money can be secure and transactions effortless.
>
> **P2P Foundation Forum Post re: "Bitcoin open source implementation of P2P currency"**
> Satoshi Nakamoto, February 2009[325]

Stablecoins are natively digital assets that seek to maintain a stable value relative to a reference asset, most often a fiat currency. Dollar-denominated stablecoins seek to combine the accessibility and frictionless use of digital assets with the stability and benefits of a dollar-based payment system. For many years, stablecoins operated in a legal gray area. But the Guiding and Establishing National Innovation for U.S. Stablecoins Act (GENIUS)[326] , which President Trump signed into law on July 18, 2025, provides regulatory clarity for this growing market, as well as incentives to bring stablecoin innovation onshore.

In the midst of debugging version 0.1.0, Satoshi sent the first test transaction of 10 bitcoin to Hal Finney, a renowned cypherpunk and early collaborator in building out the network. With the United States' long history of innovating in the payments space, it is rather fitting that the first peer-to-peer transaction employing a distributed ledger went to an American (and possibly from one, as well). With Bitcoin, Satoshi pioneered peer-to-peer transactions using digital currency. Stablecoins leverage the same technological concept to facilitate instantaneous transactions using digital dollars. GENIUS brings this groundbreaking payment technology into the financial mainstream.

U.S. consumers and businesses benefit from reliable processing of trillions of dollars of payments daily. But as Satoshi highlighted, there are inefficiencies in the legacy systems that support most of this volume. Payments, particularly retail payments, may take several days to process and ultimately settle. This lag increases the risk that one party to the transaction fails to perform (i.e., a "settlement failure") and increases costs for businesses and consumers. These inefficiencies are even more pronounced for cross-border payments, where costs are significantly higher (e.g., 6.4% for a small remittance payment in 2024) and delays significantly longer (e.g., only 33.5% of retail payments settled within one hour).[327] Technology has enabled commerce and communication to be delivered 24/7/365 globally, and Americans are increasingly looking for payments that match this ease of use and access. Distributed ledger technology (DLT) offers potential avenues to reduce these costs and delays. Stablecoins are one of the most promising DLT solutions.

GENIUS marks a watershed moment for stablecoins and digital payments. Befitting its name, GENIUS lays the regulatory groundwork for new financial rails that could significantly increase the scope and influence of the U.S. dollar system. Under President Trump's leadership, GENIUS was passed with strong bipartisan support by Congress and signed into law on July 18, 2025. The Working Group supports GENIUS and applauds Congress and President Trump for delivering this critical legislation, which will bolster the U.S. economy and cement global dollar dominance.

GENIUS establishes a clear licensing regime to ensure oversight and compliance with anti-money laundering laws and regulations. It promotes stability and transparency by requiring stablecoin issuers to maintain full reserves backed by high quality liquid assets, such as U.S. Treasuries, and to publish monthly reports of the composition of their reserves. And it protects consumers by, among other things, prioritizing stablecoin

325 satoshi, Comment to *Bitcoin open source implementation of P2P currency*, P2P Foundation (Feb. 11, 2009 at 10:27 PM), https://web.archive.org/web/20110415095236/https://p2pfoundation.ning.com/forum/topics/bitcoin-open-source.

326 S. 1582, 119th Cong. (2025) (enacted).

327 Financial Stability Board (FSB), G20 Roadmap for Enhancing Cross-Border Payments: Consolidated Progress Report for 2024 23 (Oct. 21, 2024), fsb.org/uploads/P211024-1.pdf.

holders' claims in insolvency, prohibiting issuers from rehypothecating reserves for speculative purposes, and requiring custodians of stablecoin reserves to segregate their own funds from the reserves.

GENIUS also clarifies that stablecoins are neither a security nor a commodity, opening the door to stablecoins being used for consumer payments in the United States and across the world. It encourages continued stablecoin adoption, which will reinforce the strength of the global dollar system over the coming decade. GENIUS aligns with the principles of this report and is a critical first step in establishing a comprehensive framework for the digital asset industry.

Payment Systems

Generally speaking, a payment system connects a broad range of financial institutions and customers, facilitates the movement of funds from one account to another, and includes rules and processes for transferring funds. As a simplified explanation, to make a payment, a sender must first provide instructions to a financial institution. After the instructions are received, the transaction must be "cleared" by a financial institution, such as bank or clearing house, which then facilitates the transfer of funds by performing functions such as reconciling and confirming payment details, ensuring the availability of funds, and complying with applicable regulatory requirements. Payment is then "settled" when funds are actually transferred from the sender to the recipient.

Payment systems can be either retail or wholesale. Retail payment systems are designed to process high volumes of smaller value transactions, and typically settle some hours or days after clearing. Wholesale payment systems are designed for high-value transactions and typically settle more quickly than retail payments.

Innovation in payments seeks to address inefficiencies in existing systems and provide products and services that improve customer experience. Some innovators are building solutions on top of legacy payment systems, often accessed through mobile apps. These products can offer an enhanced customer experience but, because they typically rely on legacy payment systems, may not enhance the efficiency of the underlying systems and, in some cases, may increase the number of intermediaries required to process a payment.

Both public sector and private sector actors are seeking to build new payment systems. For example, in 2017, The Clearing House, a consortium of large banks, launched an instant (real-time) payment system called RTP.[328] Since its launch, RTP has expanded to nearly 900 participating banks and conducts approximately 100 million transactions per quarter for over $160 billion.[329] In 2023, the Federal Reserve System (FRS) launched its own instant (real-time) payment system called FedNow, which, as of July 2025, has over 1,400 participating banks.[330] As was the case with the establishment of other new payment systems, such as Automated Clearing House (ACH) payments in the 1970s and 1980s,[331] initial adoption of instant payment systems has been modest due to the resources banks need to deploy to fully integrate them. Instant payment systems currently also have relatively high per transaction costs relative to ACH and other systems. Internationally, there is significant interest and experimentation across jurisdictions in building new or improving existing financial market infrastructures (FMIs) for cross-border payments or financial transactions utilizing new technologies.

Finally, institutions are also pursuing innovation in money-like payments products. Some banks are interested in offering a tokenized form of deposit that could be used as a settlement asset on existing or future payment systems. Stablecoins, likewise, are used to pay for other digital assets on trading platforms and may be used more widely in payments in the future. Blockchain or DLT-based assets present material opportunities

328 *RTP: Frequently Asked Questions*, The Clearing House, https://www.theclearinghouse.org/payment-systems/rtp/institution (last visited July 13, 2025).

329 *RTP: Real Time Payments for All Financial Institutions*, The Clearing House, https://www.theclearinghouse.org/payment-systems/rtp (last visited July 13, 2025).

330 *See FedNow Service Participants and Service Providers: Participating Financial Institutions (XLSX)*, FRBservices.org, https://www.frbservices.org/binaries/content/assets/crsocms/financial-services/fednow/fednow-live-participants.xlsx (updated July 7, 2025).

331 *See Automated Clearing House Payments*, Federal Reserve History (Sept. 28, 2023), https://www.federalreservehistory.org/essays/automated-clearing-house ("Despite high initial hopes for ACH payments, checks remained enduringly popular and ACH transaction volume remained limited for many years.").

to improve functionality in payments. Through smart contracts, payments utilizing DLT can be executed automatically when certain conditions are met. Some foreign central banks are also issuing or in the process of developing Central Bank Digital Currencies (CBDCs), with objectives varying from increasing efficiency of clearing and settlement across financial institutions to surveilling the financial activities of private citizens.

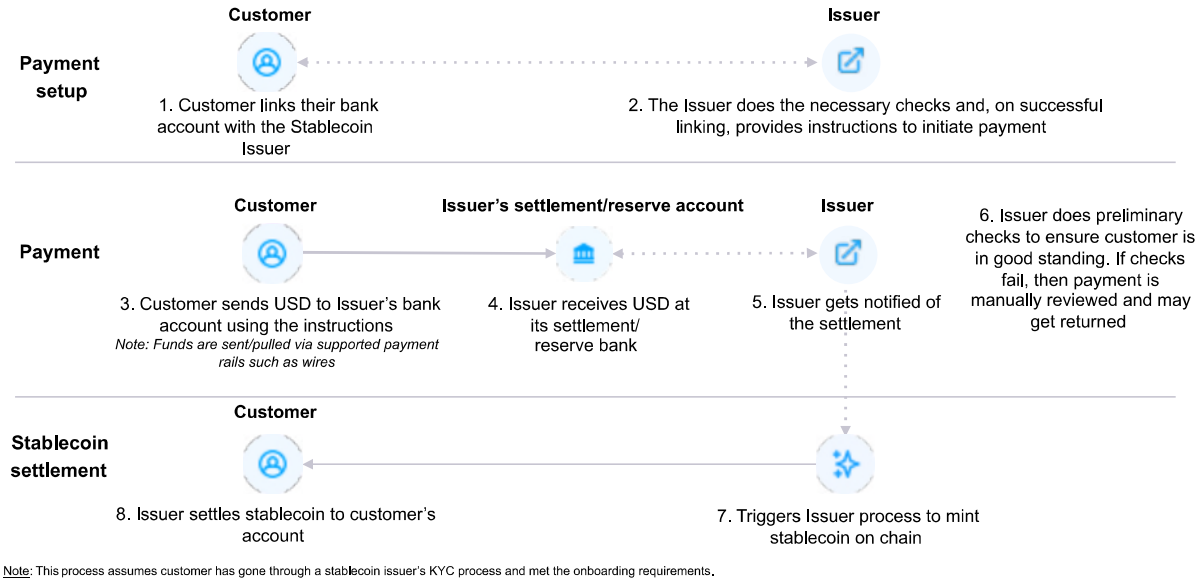
Innovations in payments have the potential to strengthen America's leadership, reduce costs for businesses and consumers, and bring the benefits of technological advancements to payments. Both domestically and internationally, the United States has the opportunity to shape the development of new payment arrangements and, through this effort, reinforce U.S. global financial leadership. If U.S. leadership is absent, new types of alternative payment arrangements could be developed that may not share U.S. interests and values and could pose risks to U.S. economic and national security.

Innovation in Payments

Stablecoins

Many stablecoins derive their value from a pool of liquid, high-quality reserve assets, but some different forms of stablecoins are backed by other types of assets (e.g., digital assets, precious metals, corporate bonds with lower credit ratings), and others attempt to maintain a stable value through pre-programmed responses to market actions rather than maintaining a pool of reserve assets (called "algorithmic stablecoins," which are typically endogenously collateralized).[332] In practice, stablecoins "pegged" to the U.S. dollar dominate the market, accounting for more than 99% of the more than $258B stablecoins outstanding by value as of July 2025, with the vast majority of issued stablecoins backed by a pool of reserve assets.[333]

Process of Minting Stablecoins[334]



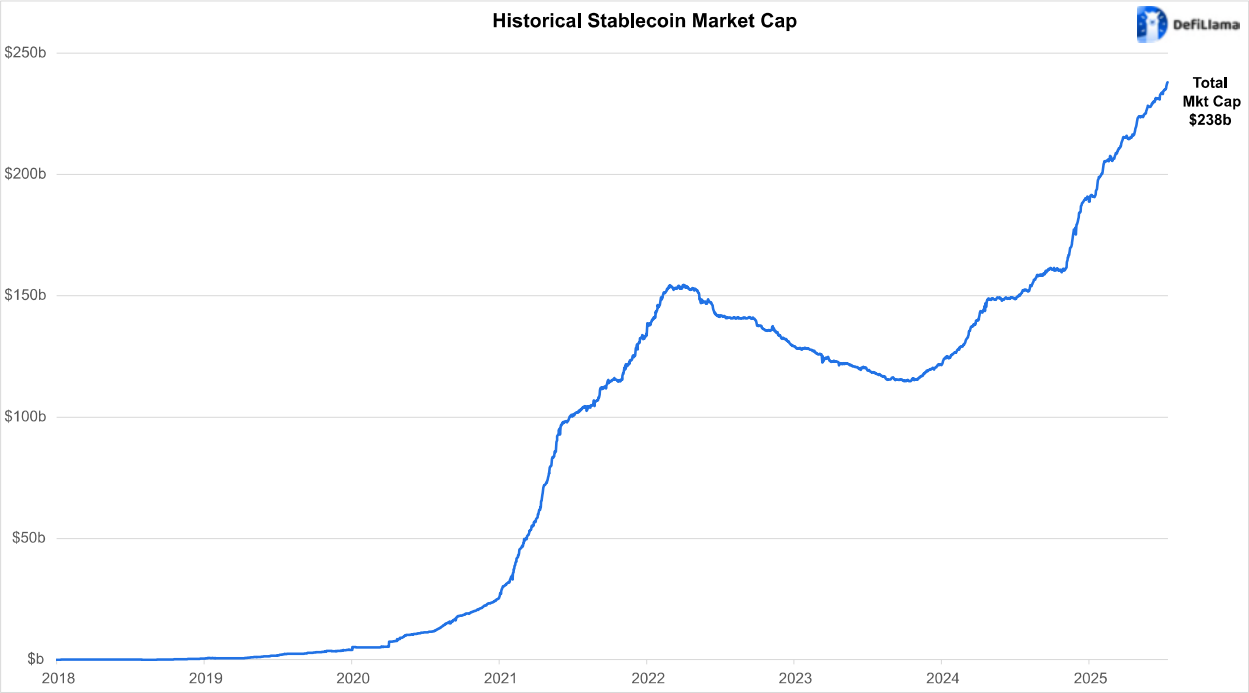
Note: This process assumes customer has gone through a stablecoin issuer's KYC process and met the onboarding requirements.

332 There are a variety of different stablecoin products. As discussed, the primary form of stablecoin is a "fiat-backed" stablecoin product that seeks to track to the U.S. dollar (e.g., USDT, USDC, BUSD, TUSD, USDP). There are also asset-collateralized stablecoins (e.g., PAXG, GLC, XAUT), crypto-collateralized/ over-collateralized stablecoins (e.g., DAI, MIM), and algorithmic stablecoins (e.g., FEI, Frax, USDN, USDD, USN) that are linked to or are redeemable for other cryptocurrencies.

333 *See Stablecoins (Filtered by Pegged USD)*, DefiLlama, https://defillama.com/stablecoins?pegtype=PEGGEDUSD (last visited July 13, 2025); *Stablecoins*, DefiLlama, https://defillama.com/stablecoins (last visited July 13, 2025).

334 Graphic prepared by Circle.

Growth in Market Capitalization of Dollar-Backed Stablecoins[335]

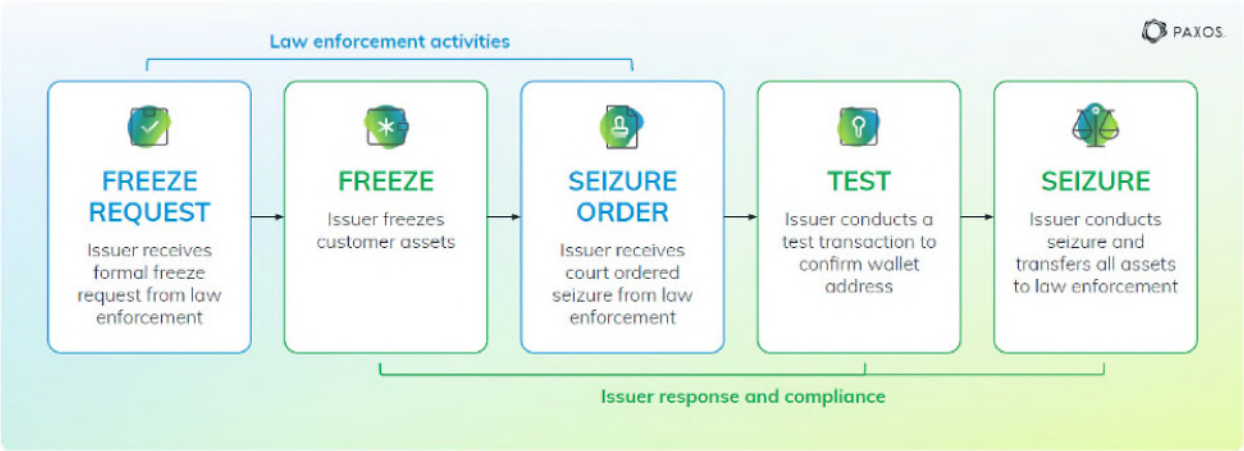


Today, stablecoins are used primarily to facilitate trading in other digital assets or to interact with smart contracts, but they could be more widely adopted as a form of payment in the future. Some stablecoin issuers have partnered with existing payment services. These partnerships seek to offer customers an alternative payment mechanism that can be used with a range of merchants and potentially offer novel features, such as programmable payments. Additionally, stablecoins could facilitate real-time peer-to-peer cross-border payments, potentially improving the current system for retail cross-border payments. Stablecoins also facilitate access to U.S. dollar denominated assets, including in areas where that access may be limited today. Stablecoin reserve assets often include U.S. Treasuries and deposits in commercial banks, which creates a connection between the traditional financial system and the digital asset ecosystem. Although stablecoins have been used in illicit finance, traditional means of money laundering and terrorist financing remain more prevalent.[336] A unique feature of stablecoins is that stablecoin issuers can coordinate with law enforcement to freeze and seize assets to counter illicit use.

335 Graphic prepared by DefiLlama. Data cover fiat-backed stablecoins (as opposed to crypto-backed or algorithmic stablecoins) that are pegged to the U.S. dollar as of July 14, 2025.

336 See U.S. Department of the Treasury (Treasury), 2024 National Terrorist Financing Risk Assessment (Feb. 2024), https://home.treasury.gov/system/files/136/2024-National-Terrorist-Financing-Risk-Assessment.pdf; U.S. Department of the Treasury, 2024 National Money Laundering Risk Assessment (Feb. 2024), https://home.treasury.gov/system/files/136/2024-National-Money-Laundering-Risk-Assessment.pdf.

Stablecoin Freeze and Seize Process[337]



Stablecoin issuers operating in the United States are generally subject to certain federal requirements, such as those stipulated under the Bank Secrecy Act (BSA).[338] Many states have also developed money transmitter frameworks under which nonbank stablecoin issuers must acquire a license. The District of Columbia,[339] Puerto Rico,[340] and all states but Montana[341] have money transmitter licensing frameworks, though various states exempt stablecoin issuers (or persons otherwise engaged exclusively in digital asset activities) from their licensing requirements.[342] Accordingly, a nonbank stablecoin issuer generally must obtain numerous licenses to operate nationwide. While states have made efforts to coordinate exams and harmonize some standards, there are significant differences in these frameworks and often overlapping supervision. Further, the lack of clarity regarding the SEC's jurisdiction over stablecoins has also limited development, including with respect to the payment of interest and ancillary services like staking. However, recent statements by SEC staff regarding stablecoins have begun to provide regulatory clarity on which types of stablecoins may fall under the agency's jurisdiction.[343] As a result, some U.S.-based issuers have sought licenses in other jurisdictions with more developed and, in some cases more stringent, regulatory frameworks.[344]

337 Graphic prepared by Paxos.

338 GENIUS explicitly subjects permitted payment stablecoin issuers to the BSA. S. 1582, 119th Cong. (2025) § 4(a)(5)(A) (enacted). More generally, domestic and foreign stablecoin issuers offering services wholly or in substantial part in the United States are treated as banks or MSBs under the BSA and its implementing regulations. *See* 31 C.F.R. § 1010.00(ff) (2024); Financial Crimes Enforcement Network (FinCEN), FIN-203-G001, Application of FinCEN's Regulations to Persons Administering, Exchanging, or Using Virtual Currencies 1 (Mar. 18, 2013), https://www.fincen.gov/sites/default/files/shared/FIN-2013-G001.pdf (stating that any person "creating, obtaining, distributing, exchanging, accepting, or transmitting virtual currencies . . . . is an MSB under FinCEN's regulations, specifically, a money transmitter, unless a limitation to or exemption from the definition applies to the person.") (emphasis omitted). Stablecoin issuers that are U.S. persons must also comply with OFAC restrictions. Finally, note that, on January 10, 2025, during the last days of the Biden Administration, the Consumer Financial Protection Bureau (CFPB) proposed a rule that would have interpreted the Electronic Fund Transfer Act and its implementing regulation, Regulation E, to apply to stablecoins. Electronic Fund Transfers Through Accounts Established Primarily for Personal, Family, or Household Purposes Using Emerging Payment Mechanisms, 90 Fed. Reg. 3723 (Jan. 15, 2025). In May 2025, the Trump Administration's CFPB withdrew the proposed rule. Protecting Americans From Harmful Data Broker Practices (Regulation V); Withdrawal of Proposed Rule, 90 Fed. Reg. 20568 (May 15, 2025).

339 D.C. Code § 26-1001 et seq.

340 10 L.P.R.A. § 2601 et seq.

341 *The Challenge of Being the Only State Not Regulating Money Transmitters*, Mont. Division of Banking & Financial Institutions (Apr. 12, 2023), https://banking.mt.gov/News/The-Challenge-of-Being-the-Only-State-Not-Regulating-Money-Transmitters.

342 *See, e.g.*, Wyo. Stat. Ann. § 40-22-104(a)(vi).

343 SEC Division of Corporate Finance, Statement on Stablecoins (Apr. 4, 2025), https://www.sec.gov/newsroom/speeches-statements/statement-stablecoins-040425. Note that GENIUS also prohibits the payment of interest or yield solely in connection with the holding, use, or retention of a payment stablecoin issued by a U.S.-licensed or foreign payment stablecoin issuer. S. 1582, 119th Cong. (2025) § 4(a)(11) (enacted).

344 For a comparison of stablecoin licensing frameworks in different countries, *see* PwC, PwC Global Crypto Regulation Report 2025 4 (Apr. 3, 2025), https://legal.pwc.de/content/services/global-crypto-regulation-report/pwc-global-crypto-regulation-report-2025.pdf.

Internationally active stablecoin issuers also face a fragmented regulatory landscape. Large financial centers are developing and implementing stablecoin frameworks. Some stablecoin firms have chosen to operate globally out of smaller jurisdictions that lack a comprehensive regulatory framework or the ability to implement one. The lack of a coherent and unified framework for stablecoins can undermine their reliability as money instruments, limiting their utility, stability, or ability to circulate without trading at a discount. It could also lead to technical challenges, as issuers attempt to meet differing standards on issues such as interoperability, privacy, and governance. Regulatory fragmentation can also lead to market fragmentation and to reduced or trapped liquidity within specific stablecoin arrangements; this can limit market depth in ways that affect the broader health of digital asset markets. More immediately, fragmentation may impose inefficient compliance and operational costs on U.S. stablecoin issuers operating internationally, damaging their competitiveness.

Stablecoins may be used in a range of applications, including retail and institutional payments and to facilitate trading in other digital assets. These use cases implicate other regulatory frameworks, including market structure,[345] which is discussed in detail in Chapter III. Customers also may rely on third-party custodians or other intermediaries to hold their stablecoins.

Recommendation

Faithfully and Expeditiously Implement GENIUS

Executive Order No. 14178 outlines the policy of the Trump Administration to promote and protect the sovereignty of the U.S. dollar, including through actions to promote the development and growth of lawful and legitimate dollar-backed stablecoins worldwide.[346] Additionally, Congress and President Trump have worked together to enact GENIUS, which enshrines a pro-innovation framework for stablecoins in Federal law.

The Working Group especially applauds the following aspects of GENIUS, which are essential to enabling growth and stability in the digital asset market.

- **Integrity of Payment Stablecoins.** The composition of reserve assets is essential to promote trust in and use of dollar-backed stablecoins. Payment stablecoins[347] are required to be backed by high-quality and liquid assets so that a claim on a stablecoin issuer representing $1 is worth $1 when redeemed. High quality and liquid reserve assets reduce the potential for losses to holders of stablecoins and the risk of a run on the stablecoin.
- **Onshore Innovation**. In order to offer or sell payment stablecoins to a person in the United States, issuers are required to retain a U.S. license – which would entitle them to modest, additional benefits – or meet comparable regulatory standards under a foreign licensing regime. Such regulation mitigates risks to U.S. financial stability, promotes U.S. national security interests, and ensures that U.S.-licensed issuers are competitive globally.
- **Facilitate Cross-Border Flows**. Internationally active stablecoin issuers may face unwarranted impediments to operating across multiple jurisdictions. GENIUS encourages cross-border flows by allowing U.S. authorities to evaluate foreign frameworks and grant reciprocity to jurisdictions with comparable or equivalent regimes. Evaluation considerations include reserve requirements, prudential standards, and supervisory and enforcement capacity.

345 Once a federal regulatory framework for stablecoins is in place, policymakers also should consider addressing the Federal income tax treatment of stablecoins. The tax rules applicable to any asset depend on how that asset is classified, (e.g., as currency, property, securities or commodities) and how returns on the assets are treated for tax purposes. The tax characterization of stablecoins is currently uncertain, which means that it is not certain which set of tax rules apply to them. For further discussion of this issue, see Chapter VII.

346 Exec. Order No. 14178, *supra* note 1, at § 1(a)(ii).

347 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).

- **Mitigate Risks to Financial System.** Risks that might undermine confidence in payment stablecoins are addressed to promote use of dollar-backed stablecoins. Specifically, the GENIUS licensing structure mitigates risks of runs (and secondary runs on underlying assets), risks of operational failure, and risks to financial stability.
- **Promote Competition.** Payment stablecoins compete with each other and with the services of other payments providers. GENIUS promotes competition and choice for consumers while recognizing differences in business models. Fostering a competitive financial ecosystem while also supporting bank (including community bank) digitalization ensures the continued relevance of both traditional financial institutions and of business models relying on new technologies.
- **Protect Consumers.** U.S.-licensed stablecoin issuers are required to address risks to consumers. They must provide adequate, monthly disclosures of reserve assets and ensure that payment stablecoin owners can redeem their stablecoins for cash 1:1 on demand. Issuers are not permitted to misrepresent that payment stablecoins are backed by the full faith and credit of the United States, guaranteed by the United States Government, or subject to federal deposit insurance or federal share insurance. Moreover, stablecoin holders' claims in insolvency are prioritized, and third parties providing custodial services for stablecoin issuers must segregate stablecoin reserves from their own assets.
- **Clarify Regulatory Status of Stablecoins.** Payment stablecoins issued by U.S.-licensed issuers (which, under GENIUS, cannot be yield-bearing) are treated as neither securities nor commodities under relevant securities and commodities laws and regulations. Additionally, U.S.-licensed stablecoin issuers are not treated as investment companies under relevant securities laws.
- **National Security.** Illicit actors, including sanctions evaders, can use stablecoins as a relatively safe and stable way to hold illicit proceeds before exchanging into fiat currency and to access U.S. dollar liquidity. In response to specific requests from U.S. and foreign law enforcement, some stablecoin issuers have, in some cases, taken steps to freeze assets. To promote integrity in stablecoins, protect U.S. national security interests, and build upon existing AML/CFT and sanctions requirements for stablecoin issuers, GENIUS explicitly treats U.S.-licensed stablecoin issuers as "financial institutions" under the BSA and therefore subject to applicable AML/CFT obligations.[348] Foreign payment stablecoin issuers are also required to comply with lawful U.S. orders to freeze and seize assets to counter illicit use.[349]

The Working Group believes that GENIUS will create a thriving and durable stablecoin ecosystem in the United States.

To enable this ecosystem to realize its full potential under GENIUS, the Working Group urges all relevant federal agencies, including Treasury, the OCC, the FDIC, the FRB, the NCUA, the SEC, and the CFTC, to faithfully and expeditiously implement GENIUS, as required by law.

Central Bank Digital Currencies

A Central Bank Digital Currency is a digital form of fiat money and direct liability of the central bank. CBDC projects around the world may be targeted at retail payments or wholesale payments. In retail usage, the CBDC targets individuals by making them holders of a liability of the central bank used for low-value transactions, including payments. In wholesale usage, the CBDC targets institutions with a function much like a tokenized central bank reserve, representing an obligation of the central bank to the token holder.

348 Note that domestic and foreign stablecoin issuers offering services wholly or in substantial part in the United States are already subject to the BSA. *Supra* note 338.

349 *See* Chapter V, "Stablecoin Freeze and Seize Process."

The Executive Order prohibits the promotion of CBDCs both domestically and abroad.[350] CBDCs are provided by a central bank government authority, and the retail use of CBDCs introduces the greatest risks to the private sector and private citizens. CBDCs consolidate government control of personal financial information, severely compromising individual economic and privacy rights. Combined with the potential incorporation of smart contracts, retail CBDCs could effectively turn fiscal policy over to unelected monetary authorities and could be used to channel resources away from certain activities and toward others at the whims of those authorities. According to one estimate, at least 90 countries are actively considering or experimenting with CBDCs.[351] China's CBDC, the e-CNY, has an expansive pilot project that involves 60 banks and payment service providers. In 2021, the European Central Bank (ECB) launched a two-year investigation phase for the issuance of a CBDC, the digital euro, and has been in the preparation phase for the digital euro's issuance since November 2023.[352] The ECB is targeting October 2025 for a Governing Council decision regarding the potential launch of the next phase in the digital euro's development.[353]

Retail CBDC efforts, both domestically and abroad, pose severe risks to individual rights, financial systems, and the sovereignty of the United States. In contrast, private sector technological innovations like stablecoins and other forms of tokenized assets preserve economic liberty.

Recommendations

- Discourage, oppose, and prohibit the ability of any agency from undertaking any action to establish, issue, or promote any CBDCs in the United States or abroad.
- Support legislation prohibiting the adoption of any CBDCs in the United States, including, for example, the Anti-CBDC Surveillance State Act, which was passed by the House of Representatives on July 17, 2025.[354]
- Support U.S. technological leadership and competitiveness in capital markets and work to upgrade domestic payment systems, FMIs, and cross-border payments; urge other countries to adopt policies that promote the role of the private sector within a technology-neutral regulatory regime.
- Examine the extent to which U.S. federal agencies (including the Banking Agencies) and relevant international financial institutions have engaged in CBDC research or pilot programs contrary to the policies set forth in Executive Order No. 14178.[355]

Promoting the Competitiveness of the U.S. Dollar Through Digital Asset Payments and Capital Markets

A promising use case for stablecoins and other new forms of money is cross-border payments and financial transactions. A wide range of jurisdictions, private sector groups, and international organizations are engaged in initiatives to improve cross-border payments.[356] Some aim to improve the current regime for cross-border payments, to which the U.S. dollar and U.S. financial institutions are central, while other projects may aim to transform global payments to the detriment of the United States.

The dollar is the leading currency in the international monetary system within which cross-border payments and financial markets have matured. The dollar's share of global trade (54%) and financial activities (59% of

350 Exec. Order No. 14178, *supra* note 1, at § 5(a) ("Except to the extent required by law, agencies are hereby prohibited from undertaking any action to establish, issue, or promote CBDCs within the jurisdiction of the United States or abroad."). The Executive Order defines "Central Bank Digital Currency" as "a form of digital money or monetary value, denominated in the national unit of account, that is a direct liability of the central bank." *Id.* at § 2(c).

351 *See Today's Central Bank Digital Currencies Status*, CBDC Tracker, https://cbdctracker.org (updated May 2025).

352 *Timeline and Progress on a Digital Euro*, European Central Bank, https://www.ecb.europa.eu/euro/digital_euro/progress/html/index.en.html (last visited July 13, 2025).

353 Staying Ahead of the Curve: Towards Further Testing and Development, European Central Bank, https://www.ecb.europa.eu/euro/digital_euro/progress/shared/pdf/241202-timeline-digital-euro-project.en.pdf (last visited July 13, 2025).

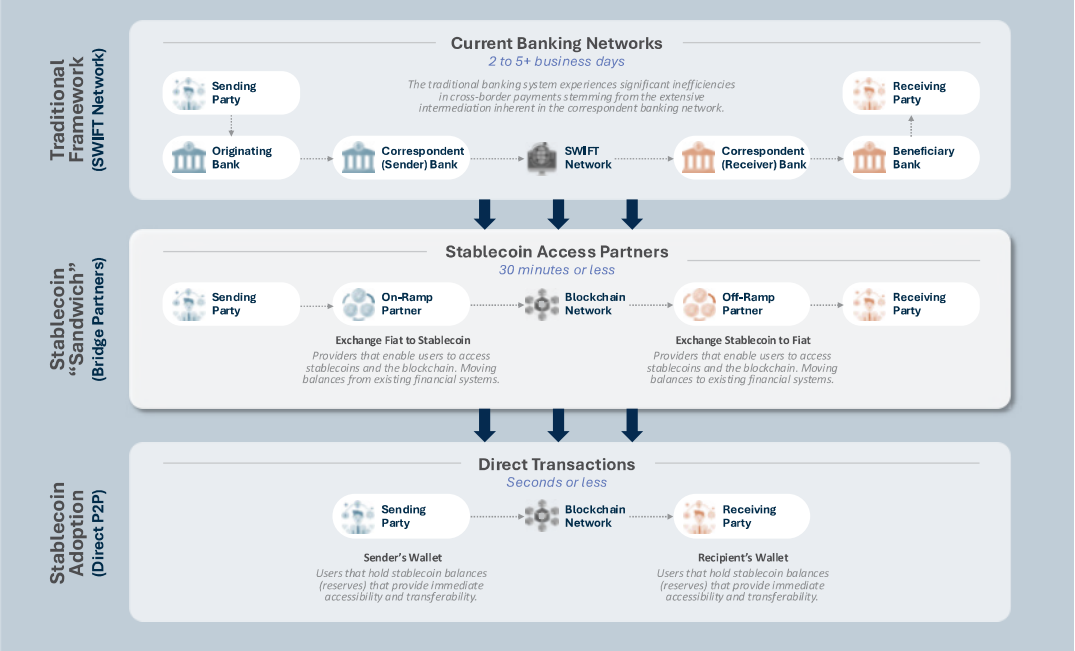
354 H.R. 1919, 119th Cong. (2025).

355 *See* Exec. Order No. 14178, *supra* note 1.

356 *See* FSB, *supra* note 327.

foreign currency reserves)[357] has been much larger than the United States' share of global Gross Domestic Product (now around 26%).[358] For example, 88% of all FX transactions use the U.S. dollar in one leg of the transaction.[359] More than 80% of the global trade finance market is denominated in dollars.[360] Around 60% of global banking sector liabilities and claims are denominated in dollars.[361] This affords the United States broad commercial and security advantages, such as reduced currency risk for U.S. businesses doing business globally. The U.S. dollar also delivers significant benefits to foreign investors, markets, and economies in the form of a stable store of value, a widely accepted retail instrument, and a highly liquid global currency, reducing transaction costs for people and businesses around the world.

Stablecoin Adoption: Converging with Existing Frameworks



Bridge to Adoption Built by "On-Ramp" & "Off-Ramp" Providers:

01 Seamless Conversion between Fiat & Stablecoin

On-ramp and off-ramp providers make it easy to convert fiat currencies into stablecoins and vice versa. This creates a smooth bridge between traditional financial systems and the crypto ecosystem, reducing barriers for users and businesses (i.e., a stablecoin "customer service").

02 No Third-Party Integration Required

These intermediary providers offer direct access to stablecoins and services without requiring external integrations. This facilitate smooth adoption but simplifying processes, enhancing key areas of security, and reducing operational complexity for businesses and users alike.

03 Integrated Regulatory Compliance Process

With built-in AML and KYC protocols, on-ramp and off-ramp providers ensure transactions are secure, transparent, and meet regulatory standards. This fosters trust among users, supports broader adoption of stablecoins, and ensures compliance with global financial regulations.

Graphic prepared by Alvarez & Marsal

357 Sam Boocker & David Wessel, *The changing role of the US dollar,* Brookings (Aug. 23, 2024), https://www.brookings.edu/articles/the-changing-role-of-the-us-dollar.

358 *GDP (current US$) – United States, World,* World Bank Group, https://data.worldbank.org/indicator/NY.GDP.MKTP.CD?end=2024&locations=US-1W&start=1960&view=chart (last visited July 13, 2025).

359 U.S. Department of the Treasury Under Secretary for International Affairs Jay Shambaugh, Remarks at the Third Conference on the International Roles of the U.S. Dollar Hosted by the Federal Reserve Board and the Federal Reserve Bank of New York (May 20, 2024), https://home.treasury.gov/news/press-releases/jy2352.

360 First Deputy Managing Director Gita Gopinath, International Monetary Fund, *Geopolitics and its Impact on Global Trade and the Dollar*, International Monetary Fund (May 7, 2024), https://www.imf.org/en/News/Articles/2024/05/07/sp-geopolitics-impact-global-trade-and-dollar-gita-gopinath.

361 Carol Bertaut, Bastian von Beschwitz & Stephanie Curcuro, *"The International Role of the U.S. Dollar" Post-COVID Edition,* Board of Governors of the Federal Reserve System: FEDS Notes (June 23, 2023), https://www.federalreserve.gov/econres/notes/feds-notes/the-international-role-of-the-us-dollar-post-covid-edition-20230623.html.

International payments are mainly conducted via the correspondent banking system, in which the primary participants are large banks and financial intermediaries with access to U.S. dollar clearing services and liquidity. Smaller institutions typically access this system through accounts at larger banks. Participants send payment instructions and confirmations through specialized messaging systems, like that operated by the Society for Worldwide Interbank Financial Telecommunication (SWIFT). Payments ultimately settle on commercial and central bank balance sheets, often on a net basis at predetermined times of day for reasons of operational and liquidity efficiency. A single payment may travel across several bank balance sheets and require reconciliation all along the chain in a complex system that has evolved over decades. In many FX transactions between two non-U.S. currencies, the original currency is converted first to U.S. dollars and then to the final currency, because it is often cheaper than a direct conversion or because there is higher liquidity for conversion to or from the U.S. dollar. This explains the U.S. dollar's dominant role in FX transactions, and why U.S. institutions and U.S. dollar accounts are central to cross-border payments. This centrality incentivizes foreign financial institutions to implement U.S. sanctions and maintain robust AML/CFT controls, both of which are key U.S. economic and national security tools.

For individuals sending remittances, especially to countries with poorer connectivity to the correspondent banking system, payments may be slower, more expensive, and more opaque. According to 2024 World Bank data, the global average cost of remitting $200 was 6.4%, with high variation across regions and only 77% of remittances were available within one day.[362] Such direct and indirect costs impede economic development, creating a demand for alternatives that may be filled by U.S. adversaries. Additionally, as capital markets accelerate, slower payment infrastructure could increase the risk of failed transactions and may increase costs for securities firms active across global markets. Despite next day (T+1) settlement for most securities transactions in the United States, FX transactions still settle in two days (T+2), requiring banks to hold capital against FX transactions to insure against settlement failure. Additionally, large sections of the system may have dependencies on unreliable core infrastructures, introducing concentration and operational risks. For example, in late February 2025, a "hardware defect" in Europe's Target 2 legacy payment system caused a seven-hour outage, delaying trillions of euros worth of payments.[363] Finally, foreign jurisdictions, seeking to evade U.S. sanctions, may seek to create alternatives that avoid U.S. jurisdiction.

Digital asset proponents are applying the full suite of new money-like products to cross-border retail payments. Digital assets and stablecoins already flow across borders, although the evidence indicates that, except for in select countries, these flows predominantly finance activity within the global digital asset ecosystem.[364]

Large-value wholesale cross-border payments can also benefit from the advantages of digital assets and DLT. While some of this work advances piecemeal upgrades or technical improvements to existing systems, there is significant interest in designing new multilateral FMIs or common platforms for cross-border payments. In its most ambitious form, a new FMI would accommodate varied types of tokenized assets traded across borders. Development of new FMIs remains conceptual for now, and further exploration is ongoing to determine the technical, operational, and economic viability. The ability to instantaneously transfer deposits globally, or to program payments with specific conditions, has the potential to significantly enhance client firms' treasury operations and cash management. Atomic settlement of wholesale FX payments could also help significantly reduce settlement risk. Private sector financial institutions, including U.S. firms, both individually and in consortia, are driving some of these projects.

362 FSB, *supra* note 327, at 33.

363 Tom Simms, Francesco Canepa & John O'Donnell, *ECB's multi-trillion payments breakdown sends shudders through Europe*, (Feb. 28, 2025), https://www.reuters.com/markets/europe/deutsche-boerses-clearstream-deals-with-residual-impact-ecb-outage-2025-02-28.

364 Raphael Auer et al., *DeFiying gravity? An empirical analysis of cross-border Bitcoin, Ether and stablecoin flows*, BIS Working Paper No. 1265 (May 2025), https://www.bis.org/publ/work1265.pdf.

Without strong U.S. leadership, the development of alternative payment arrangements may weaken the role of U.S. financial institutions, the dollar, and the effectiveness of U.S. national security tools. While many private sector projects are being led by or involve U.S. financial institutions, many have based their innovation outside the United States to take advantage of more favorable regulatory environments for deploying digital assets and tokenization. This reduces the United States' ability to establish, influence, and benefit from new standards and best practices for innovative cross-border FMIs. Additionally, adversarial nations have been active in efforts to establish new cross-border payment arrangements with the explicit goal of reducing reliance on U.S. dollar-based infrastructures. The negative effects of these efforts could build as more arrangements are created from which the U.S. dollar and the United States are absent. Advances in international projects to develop FMIs using novel payment technology may define new de facto standards. If the United States does not lead, these standards may be of poor quality, conflict with U.S. values or national security priorities, or intentionally erode U.S. interests.

The United States must seize the opportunity to exert leadership over the emergence and evolution of new financial market technologies and champion the U.S. private sector to lead these innovations. U.S. participation in the development of alternative payment arrangements—either directly or indirectly through the oversight of U.S. private sector initiatives—will help preserve the dollar's role and increase the ability of the United States to preserve or improve the efficacy of its national security tools. For example, a U.S. regime for well-regulated stablecoins that can flow across borders via reciprocity arrangements, as is envisioned by GENIUS, can support the emergence of a new U.S.-based system for real-time cross-border dollar payments. By virtue of the dollar's availability, other U.S.-led arrangements that may rely on innovations such as tokenization would be relatively more attractive than competing non-dollar models. The involvement of U.S. financial institutions would also reinforce U.S. AML/CFT and sanctions frameworks, incentivize foreign financial institutions to maintain strong AML/CFT programs, and incentivize non-U.S. persons to abide by U.S. sanctions if they seek to access to the U.S. financial system.

Recommendations

- Relevant U.S. agencies, including Treasury, should promote U.S. private sector leadership in the responsible development of innovative cross-border payments and financial markets technologies. Toward this end, Treasury should consider using its convening authority to encourage and provide clarity to U.S. financial institutions in leading these efforts.
- Treasury and other relevant agencies should 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. Standards, including international standards, should be calibrated to accurately reflect the risk of innovative digital products and services.
- Domestically and internationally, U.S. authorities should encourage payment solutions that: (i) protect the two-tier banking system and promote the private sector's role in financial intermediation, payments, and capital formation; (ii) preserve individual rights and limit government control of personal financial information; and (iii) incorporate robust and effective AML/CFT and sanctions controls.
- Treasury, in coordination with other relevant agencies, should engage with international counterparts and institutions by leading initiatives to upgrade domestic payment systems, FMIs, and cross-border payment systems, to help protect the primacy of the dollar-based international monetary system.

CHAPTER VI

Countering Illicit Finance

Countering Illicit Finance

> "The developers expect that this will result in a stable-with-respect-to-energy currency outside the reach of any government." – I am definitely not making an *[sic]* such taunt or assertion.
>
> **BitcoinTalk Forum Post Re: "Slashdot Submission for 1.0"**
> Satoshi Nakamoto, July 2010[365]

Digital assets, like traditional assets, are subject to abuse by bad actors—terrorists, drug traffickers, state-sponsored hackers, human traffickers, fraudsters, sanctions evaders, and others. But unlike traditional assets, the technology underlying digital assets enables ways to mitigate the risk of illicit transactions.[366] The U.S. financial system's strength, size, and reliability make it a notable target, and misuse by these actors affects matters of national security. To unleash the full potential of digital assets in the United States, preserve the rights of innovators to build technologies that advance individual privacy and liberty, and stop financial crime that targets Americans, the Working Group encourages the adoption of certain measures to deter and combat illicit finance.

These measures, tools, and authorities must be properly scoped to encourage innovation, respect the liberties and privacy of lawful digital asset users, and protect the financial system from abuse. Treasury's policy, enforcement, intelligence, and regulatory tools under the Bank Secrecy Act (BSA)[367] and sanctions authorities are critical to protecting the U.S. financial system. Effective and clear regulation coupled with law enforcement actions against malicious actors can build confidence among U.S. users and firms seeking to grow domestically. Transparency regarding developers' obligations under the law will encourage the onshoring of blockchain development and support the efforts of American innovators to lead the digital assets industry forward.

The Financial Crimes Enforcement Network (FinCEN), a Treasury bureau tasked with safeguarding the financial system from illicit activity, has shown leadership on this front. As part of an ongoing effort to establish clarity for the digital asset industry and the Trump Administration's broader efforts to ensure regulations are fit-for-purpose, FinCEN is withdrawing two notices of proposed rulemaking related to digital assets, including one rulemaking colloquially referred to as the "unhosted wallet rule"[368] and a second that proposed amendments to the travel and recordkeeping rules.[369]

The U.S. Department of Justice (DOJ) has also committed to ending the Biden Administration's strategy of regulation by prosecution in the digital assets space.[370] The DOJ will no longer pursue litigation or enforcement actions that have the effect of superimposing regulatory frameworks on digital assets.[371] This decision stems from the fact that financial regulators (including the SEC, and the CFTC) have regulatory subject matter expertise and are better suited for such regulatory activities.[372] Going forward, the DOJ's investigations and prosecutions involving digital assets shall focus on prosecuting individuals who victimize digital asset investors or

365 satoshi, *supra* note 16.

366 *Supra* note 349

367 The term "Bank Secrecy Act" refers to a collection of statutes, including certain parts of the Currency and Foreign Transactions Reporting Act, Pub. L. No. 91-508, its amendments, and the other statutes relating to the subject matter of that Act. These statutes are codified at 12 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).

368 *See* Requirements for Certain Transactions Involving Convertible Virtual Currency or Digital Assets, 85 Fed. Reg. 83840 (Dec. 23, 2020).

369 *See* Threshold for the Requirement To Collect, Retain, and Transmit Information on Funds Transfers and Transmittals of Funds That Begin or End Outside the United States, and Clarification of the Requirement To Collect, Retain, and Transmit Information on Transactions Involving Convertible Virtual Currencies and Digital Assets With Legal Tender Status, 85 Fed. Reg. 68005 (Oct. 27, 2020).

370 U.S. Department of Justice (DOJ), Memorandum from the Deputy Attorney General: Ending Regulation by Prosecution 1 (Apr. 7, 2025), https://www.justice.gov/dag/media/1395781/dl?inline.

371 *Id.*

372 *Id.* at 1, 3.

use digital assets in furtherance of criminal offenses.[373] The DOJ has also disbanded its National Cryptocurrency Enforcement Team and refocused its Market Integrity and Major Frauds Unit on other priorities.[374]

The Working Group applauds these actions and encourages all relevant agencies to follow the examples set by FinCEN and the DOJ in evaluating and better tailoring regulation and enforcement.

Illicit Finance Risks

U.S. digital asset participants use digital assets for a variety of legitimate purposes, including investments, remittances, and payment for goods and services. However, like any medium of exchange, digital assets may be used by illicit actors to facilitate and profit from crime. The ability to transfer assets quickly across borders and perceptions of anonymity, which appeal to many digital asset users, also make digital assets attractive to illicit actors.

Despite increasing over the last decade, the prevalence of money laundering and terrorist financing via digital assets remains well below that of the same activities utilizing fiat currency, bank and traditional money services fund transfers, and other methods that do not involve digital assets.[375] The Federal government's approach to addressing illicit finance in the digital asset ecosystem is informed by an understanding of how threat actors misuse digital assets and the features of the underlying technology. Moreover, certain industry estimates indicate that the vast majority of digital asset activity is legitimate, with a relatively small amount of illicit activity. For example, two blockchain analytics companies assessed that between 0.61% and 0.86% of all onchain digital asset volumes in 2023 were illicit, accounting for between $46.1 billion and $58.7 billion. As indicated below, these companies have also conducted assessments for 2024 but anticipate adjustments to illicit volume over time with delayed reporting, further analysis, and improved attribution techniques to identify illicit activity.[376] These assessments help provide a baseline for illicit activity in the digital asset ecosystem given certain limitations with using blockchain information for ecosystem-wide trends.[377]

373 *Id.* at 1.

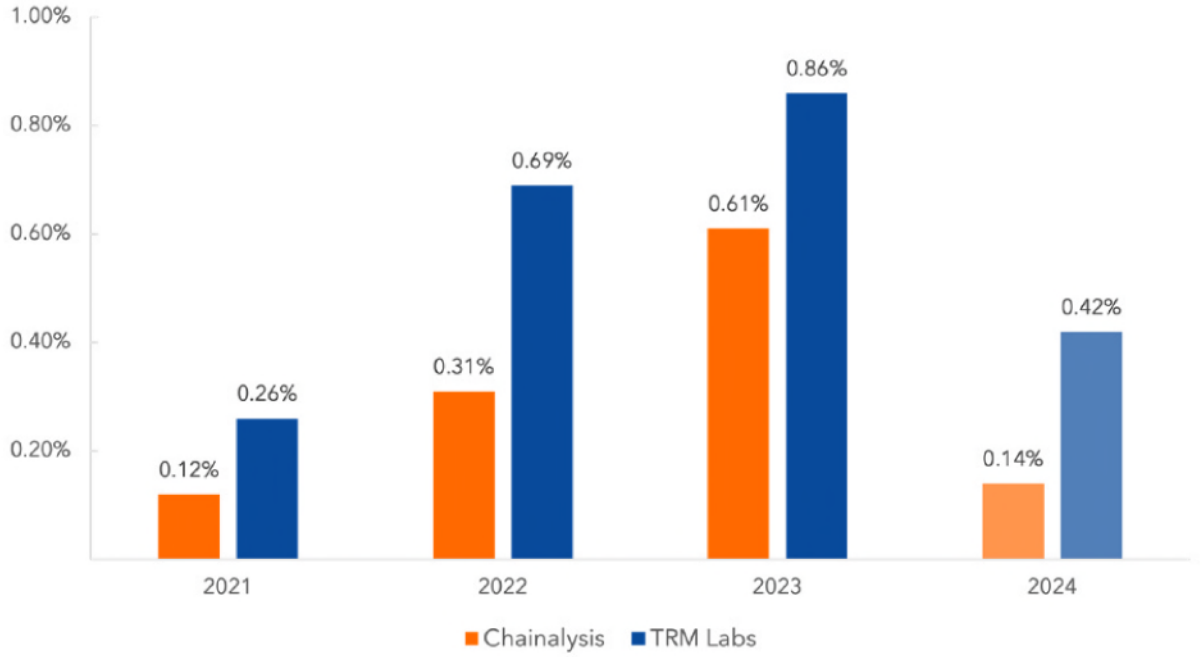
374 *Id.* at 4.

375 *See* Treasury, 2024 National Terrorist Financing Risk Assessment, *supra* note 336; Treasury, 2024 National Money Laundering Risk Assessment, *supra* note 336.

376 Chainalysis, The 2025 Crypto Crime Report 5 (Feb. 2025), https://www.chainalysis.com/wp-content/uploads/2025/03/the-2025-crypto-crime-report-release.pdf; TRM Labs, 2025 Crypto Crime Report 4 (2025), https://cdn.prod.website-files.com/6082dc5b670562507b3587b4/6823baf9045160ea474b3f7a_TRM_2025%20Crypto%20Crime%20Report.pdf.

377 The limitations include the adjustments described above, variations in how analytic companies attribute illicit activity to wallets, differences in the networks and assets included in the assessment, and the fact that assessments only include transactions involving wallet addresses that have been identified as illicit. Attribution for these purposes can be particularly challenging for transactions involving proceeds of crimes initially conducted in fiat currency and subsequently converted into digital assets.

Share of Digital Asset Transaction Volume Associated with Illicit Activity, 2021-2024[378]



Notably, in addition to volume of illicit activity, the harmful impact of illicit conduct must also be considered in assessing illicit finance risks in the digital asset ecosystem. For example, while the Democratic People's Republic of Korea's (DPRK) revenue generation through digital assets is a small amount compared to the market capitalization of digital assets, DPRK is reliant on digital assets to fund the regime's weapons of mass destruction and ballistic missiles program.[379]

DPRK and ransomware cybercriminals have generated significant revenue in digital assets through theft and extortion payments for several years. In February 2025, DPRK cybercriminals stole digital assets valued at $1.5 billion from a digital asset service provider, the largest theft in digital asset history.[380] In 2024, reported losses from digital assets fraud exceeded $9 billion, a 66% increase from 2023, according to complaints received by the Federal Bureau of Investigation's (FBI's) Internet Crime Complaint Center.[381] Losses to digital asset investment schemes accounted for nearly $6 billion of this total amount.[382]

Illicit actors can exploit several vulnerabilities in the digital asset ecosystem, including jurisdictional arbitrage, digital asset service providers that fail to comply with applicable AML/CFT and sanctions obligations, and anonymity-enhancing technologies. Often, illicit actors use foreign digital asset service providers with weak AML/CFT and sanctions requirements to launder illicit proceeds. Some of these service providers tout their weak AML/CFT and sanctions controls to attract customers. The lack of standardization across AML/CFT frameworks across jurisdictions allows some digital asset service providers to operate in countries with deficient or non-existent AML/CFT requirements. A Financial Action Task Force (FATF) survey identified that as of mid-2025, nearly 30 countries had not determined their approach to digital asset service providers for AML/CFT, and many countries

378 Chainalysis, *supra* note 376; TRM Labs, *supra* note 376.

379 *See* Office of the Director of National Intelligence, Annual Threat Assessment of the U.S. Intelligence Community (Mar. 2025), https://www.dni.gov/files/ODNI/documents/assessments/ATA-2025-Unclassified-Report.pdf.

380 Federal Bureau of Investigation (FBI), I-022625-PSA, North Korea Responsible for $1.5 Billion ByBit Hack (Feb. 26, 2025), https://www.ic3.gov/psa/2025/psa250226.

381 FBI, Federal Bureau of Investigation Internet Crime Report 2024 35 (2024), https://www.ic3.gov/AnnualReport/Reports/2024_IC3Report.pdf.

382 *Id.* at 36.

with AML/CFT frameworks for digital asset service providers have not yet operationalized them.[383] These international gaps may allow non-compliant digital asset service providers outside the United States to solicit U.S. customers away from more compliant U.S.-based digital asset service providers.

Even in the United States, where digital asset service providers are subject to AML/CFT and sanctions obligations, some digital asset service providers fail to comply with applicable obligations. Such compliance failures can result in an uneven playing field, placing firms that faithfully discharge their responsibilities to help safeguard the U.S. financial system at a competitive disadvantage.

Illicit actors use certain tools and methods—such as mixers, anonymity-enhanced cryptocurrencies (AECs), and chain-hopping—to obfuscate transactional information that may be otherwise viewable on public blockchains.[384] These tools and methods can hinder law enforcement investigations, including tracing criminal proceeds for seizure and forfeiture, which can allow victim compensation. While these methods and tools may also be used for legitimate digital assets activities, including by users who want increased privacy for digital asset transactions (see Chapter VI, Advancing Privacy through Digital Identity and Related Tools), they can heighten illicit finance risks if they do not simultaneously allow for or promote risk mitigation measures.

Illicit actors may also use DeFi services, along with self-custody, to facilitate peer-to-peer transactions in the laundering process. While there are licit reasons to self-custody digital assets (see Chapter II), illicit actors can use the pseudonymity of self-custody and peer-to-peer payments to conceal or to quickly move proceeds.

Improving the AML/CFT and Sanctions Frameworks

The U.S. AML/CFT and sanctions frameworks are designed to protect the integrity of the U.S. financial system on which U.S. persons and the global economy rely for trade, investments, remittances, and everyday transactions. The BSA, administered by FinCEN, places obligations on financial institutions to monitor, report, and take steps to mitigate money laundering, the financing of terrorism, and other illicit finance activity. These requirements both mitigate the risk of illicit actors accessing the financial system and provide actionable information for law enforcement and national security agencies to identify and disrupt criminal activity. U.S. economic and trade sanctions, administered by Treasury's Office of Foreign Assets Control (OFAC), prohibit certain adversaries from accessing the U.S. financial system and deter or disrupt behavior that undermines U.S. national security or foreign policy through the imposition of material costs.

To implement the Trump Administration's policy of encouraging innovation and responsible use of digital assets, the United States must protect the digital asset ecosystem and its users by mitigating and combatting the risks posed by illicit use. Meeting this objective requires AML/CFT and sanctions regimes that impose clear obligations, tailored to the risk and structure of the industry. In the view of the Working Group, this moment serves as a valuable opportunity to comprehensively review the AML/CFT regime to ensure it protects the financial system from abuse without impeding on the rights of law-abiding Americans. Such regulatory frameworks should respect the lawful use of digital assets by individuals and digital asset firms in the United States and acknowledge Americans' privacy rights. Updates to the AML/CFT and sanctions regimes to better account for digital asset actors will create a more transparent, resilient, and safe digital asset sector and give the United States a comparative advantage globally.

383 Financial Action Task Force, Targeted Update on Implementation of the FATF Standards for Virtual Assets and Virtual Asset Service Providers 11 (Jun. 2025), https://www.fatf-gafi.org/content/dam/fatf-gafi/recommendations/2025-Targeted-Upate-VA-VASPs.pdf.coredownload.pdf.

384 "Chain-hopping" refers to the practice of converting one digital asset into a different digital asset at least once before moving the funds to another service or platform.

Prescribing BSA Obligations

BSA Background

The BSA authorizes the Secretary of the Treasury to impose various obligations on financial institutions to detect and combat money laundering, the financing of terrorism and other illicit finance activity, and to otherwise safeguard the national security of the United States.

Among other things, the BSA and its implementing regulations require financial institutions to establish written programs to combat money laundering and the financing of terrorism and to keep records[385] and file reports that "are highly useful in . . . criminal, tax, or regulatory investigations, risk assessments, or proceedings" or "intelligence or counterintelligence activities, including analysis, to protect against terrorism."[386] The Secretary of the Treasury may also "establish appropriate frameworks for information sharing among financial institutions and service providers, their regulatory authorities, associations of financial institutions, the Treasury, and law enforcement authorities to identify, stop, and apprehend money launderers and those who finance terrorists."[387]

In 2021, Congress enacted the Anti-Money Laundering Act of 2020 (AML Act) as a part of the William M. (Mac) Thornberry National Defense Authorization Act for Fiscal Year 2021.[388] A key objective of the AML Act was to strengthen and modernize the AML/CFT regulatory framework. The AML Act also amended the BSA to further solidify the inclusion of digital assets into the U.S. AML/CFT framework, expanding key definitions to account for "value that substitutes for currency."[389] The Secretary of the Treasury has delegated the authority to implement, administer, and enforce the BSA and its implementing regulations to the Director of the FinCEN.

An entity generally has BSA obligations if it qualifies as a "financial institution" under the BSA, which is based on the entity's activities, regardless of whether the activity is in fiat, digital assets, or both. Participants in the digital asset ecosystem may meet the definition of one or more financial institution types under the BSA (e.g., MSBs, insured banks, trust companies, futures commissions merchants, broker-dealers), but are predominantly treated as MSBs.[390] Key components of regulations implementing the BSA pre-date the creation of digital assets, smart contracts, and other industry innovations. Accordingly, the current U.S. AML/CFT framework does not clearly account for all aspects of the digital asset ecosystem.

Statutory Changes for Digital Asset Financial Institutions

The U.S. AML/CFT framework should consider how obligations can be better tailored and clarified for digital asset actors. To achieve this, the Working Group recommends that Congress—as it considers germane legislation—consider providing statutory changes to the BSA that define with greater certainty the actors in the

385 *See* 31 U.S.C. § 5318(h). The program rules are located at 31 C.F.R. §§ 1020.210 (banks), 1021.210 (casinos and card clubs), 1022.210 (money services businesses), 1023.210 (brokers or dealers in securities, or broker-dealers), 1024.210 (mutual funds), 1025.210 (insurance companies), 1026.210 (futures commission merchants and introducing brokers in commodities), 1027.210 (dealers in precious metals, precious stones, or jewels), 1028.210 (operators of credit card systems), 1029.210 (loan or finance companies), and 1030.210 (housing government sponsored enterprises) (2024). Additionally, under Title 12 of the U.S. Code, the federal banking agencies and the NCUA maintain regulations requiring insured depository institutions and credit unions to "establish and maintain procedures reasonably designed to assure and monitor" their compliance with the requirements of the BSA. *See, e.g.*, 12 U.S.C. §§ 1818(s), 1786(q); *see also* 12 C.F.R. §§ 208.63(b), 211.5(m), 211.24(j) (FRB); 12 C.F.R. § 326.8(b) (FDIC); 12 C.F.R. § 748.2 (NCUA); 12 C.F.R. § 21.21(c) (OCC) (2025).

386 31 U.S.C. §§ 5311(1), 5318(g) (2024).

387 31 U.S.C. §§ 5311(5) (2024); *see also* 31 U.S.C. § 310(d) (2024).

388 Pub. L. No. Law 116-283 (2021). The AML Act was enacted as Division F, §§ 6001-6511, of the Pub. L. No. 116-283 (2021).

389 *See* AML Act § 6102(d). Note that regulatory definitions pre-dating the AML Act recognized that BSA obligations could apply to activity involving "value that substitutes for currency." *See* Financial Crimes Enforcement Network; Amendments to the Bank Secrecy Act Regulations-Definitions and Other Regulations Relating to Money Services Businesses, 74 Fed. Reg. 22129, 22137 (May 12, 2009) (discussing current definition of "money transmitter" and proposed inclusion of "value that substitutes for currency," among other changes"); Bank Secrecy Act Regulations – Definitions and Other Regulations Relating to Money Services Businesses, 76 Fed. Reg. 43585 (July 21, 2011) (adopting definition); FinCEN, FIN-2019-G001, Application of FinCEN's Regulations to Certain Business Models Involving Convertible Virtual Currencies 4 (May 9, 2019), https://www.fincen.gov/sites/default/files/2019-05/FinCEN%20Guidance%20CVC%20FINAL%20508.pdf; FinCEN, FIN-2013-G001, *supra* note 338, at 3.

390 *See, e.g.*, 31 C.F.R. §§ 1010.100(h) (defining broker or dealer in securities), 1010.100(bb) (defining introducing broker-commodities), 1010.100(ff) (defining money services business) (2024); Tarbert, Blanco & Clayton, *supra* note 111.

digital asset ecosystem that are subject to BSA obligations. Such legislation could consider creating a bespoke digital asset-specific financial institution types or sub-types, which could enable Treasury to more carefully tailor AML/CFT obligations to different participants in the digital asset industry, such as exchanges, stablecoin issuers, and firms engaged in digital commodity transactions.

While stablecoin issuers typically transact with institutional rather than retail customers, illicit actors may use stablecoins to generate and launder their proceeds of crime. As a good practice, some issuers have capabilities to mitigate risks related to secondary market transactions in the stablecoin that they issue. This can include the ability to freeze funds or block transactions involving their stablecoin. Many issuers also use blockchain analytics to identify risks in the stablecoin ecosystem and can use that information to freeze tokens when warranted. Additionally, Treasury should work to develop tailored AML/CFT obligations for payment stablecoin issuers, including ensuring that U.S. law enforcement receives highly useful reports involving stablecoins. Treasury should also explore how stablecoin issuers' risk-based AML programs should address higher-risk activities in the secondary stablecoin ecosystem without placing undue burden on the issuer, as well as program requirements relating to freezing and seizing stablecoins. Chapter V discusses additional information on stablecoins and related regulatory recommendations that are relevant for understanding the operational context in which stablecoins are used.

Further, as discussed in Chapter III, certainty regarding the regulatory market structure for digital assets is critical to market growth. As Congress considers updating federal agencies' authorities related to digital assets, it should ensure that necessary changes are also codified in the BSA such that digital asset firms supervised by the CFTC and SEC, including any newly created types of financial institutions, are subject to BSA obligations as appropriate.

BSA Obligations and Considerations for DeFi

FinCEN has taken steps to promote certainty and foster innovation in the digital markets. Guidance from FinCEN has been useful in assisting industry with understanding obligations as money transmitters. In 2013, FinCEN issued guidance, which explained how FinCEN characterized certain activities involving digital assets under the BSA and implementing regulations.[391] The guidance clarified that an administrator or exchanger that "(1) accepts and transmits a virtual currency or (2) buys or sells convertible virtual currency for any reason" is a money transmitter[392] under FinCEN regulations and, therefore, subject to the regulations of a money services business (MSB) under the BSA.[393] The 2013 guidance also stated that a user who "obtains virtual currency and uses it to purchase real or virtual goods or services is not an MSB under FinCEN's regulations."[394]

In 2019, FinCEN issued additional guidance on the application of regulations on certain business models involving convertible virtual currencies (CVCs).[395] The guidance highlighted key facts and circumstances FinCEN used to set forth how various models could be treated under the BSA. For example, the guidance further clarified how FinCEN regulations may apply to peer-to-peer activity, explaining that "Peer-to-Peer (P2P) exchangers are (typically) natural persons engaged in the business of buying and selling CVCs," and

391 FinCEN, FIN-2013-G001, *supra* note 338.

392 *Id.* at 3. FinCEN's regulations define "money transmitter" as a person that provides money transmission services, or any other person engaged in the transfer of funds. 31 C.F.R. § 1010.100(ff)(5)(i)(A) (2024). The term "money transmission services" means "the acceptance of currency, funds, or other value that substitutes for currency from one person and the transmission of currency, funds, or other value that substitutes for currency to another location or person by any means." *Id.*

393 FinCEN, FIN-2013-G001, *supra* note 338, at 3. The guidance also defines "virtual currency" as "a medium of exchange that operates like a currency in some environments, but does not have all the attributes of real currency" and notes that "virtual currency does not have legal tender status in any jurisdiction." *Id.* at 1. The guidance defines convertible virtual currency (CVC) as "a type of virtual currency [that] either has an equivalent value in real currency, or acts as a substitute for real currency." *Id.* Later guidance from FinCEN refers to "digital asset," "cryptocurrency," and "cryptoasset" as labels applied to particular types of CVCs. *See* FinCEN, FIN-2019-G001, *supra* note 389, at 7.

394 FinCEN, FIN-2013-G001, *supra* note 338, at 2.

395 FinCEN, FIN-2019-G001, *supra* note 389.

that a "natural person operating as a P2P exchanger that engages in money transmission services involving real currency or CVCs must comply with BSA regulations as a money transmitter acting as a principal."[396] In contrast, "a natural person engaging in such activity on an infrequent basis *and* not for profit or gain would be exempt from the scope of money transmission."[397]

FinCEN's 2019 guidance also provided insight on how an entity's control over access to value could impact whether an entity is an MSB. The guidance set forth four criteria to be considered an intermediary under the BSA, including "whether the person acting as intermediary has total independent control over the value."[398] Hosted wallet providers are generally subject to BSA requirements since they control the user's value.[399] In contrast, in unhosted, single-signature wallets, the owner has "total independent control over the value," and, according to the guidance, a natural person who engages in peer-to-peer transactions for their own purposes is not a money transmitter.[400]

Finally, the guidance suggests that determining whether certain participants in the DeFi ecosystem provide money transmission services depends on the facts and circumstances of the model, which would presumably also include a consideration of whether the service exerts "total independent control."[401] FinCEN further stated in an administrative ruling that "production and distribution of software, in and of itself, does not constitute acceptance and transmission of value, even if the purpose of the software is to facilitate the sale of virtual currency."[402]

While this guidance is instructive, the current U.S. AML/CFT regime does not sufficiently consider truly decentralized protocols, where the governance/decision-making is distributed across communities of users, and the protocols may be immutable or otherwise technologically incapable of collecting customer information or reporting suspicious activities. The uniqueness of the DeFi ecosystem has propelled a protracted conversation in policy circles across the globe regarding the appropriateness and logistics of requiring decentralized protocols and other participants in the DeFi ecosystem to adhere to same AML/CFT obligations as centralized intermediaries, whether unique obligations tailored to the technology should be developed, and how to effectively mitigate illicit finance risks in the DeFi ecosystem, among other core considerations.

This challenge calls for creative solutions to enable clarity for those engaged with the technology. Decentralized protocols generally have no administrator, retain no control over any funds or digital assets being transacted, are unable to collect customer information, and cannot file Suspicious Activity Reports (SARs). Moreover, decentralized protocols are unable to complete simple MSB registration functions, like completing the registration process with FinCEN—Form 107—that necessitates importing identity validating information (i.e., SSN/EIN, phone numbers, physical address, etc.), or conducting entity-level MSB anti-money laundering obligations, such as adopting a written anti-money laundering program.[403]

To provide clarity to industry and allow tailored solutions to mitigate illicit finance risks, Congress should consider a principled approach to defining various actors in the DeFi ecosystem as discussed in Chapter III. Congress could provide a clear definition of what constitutes "true" decentralized protocols and clarify, or provide direction to the appropriate regulator to clarify, how obligations apply to entities that utilize smart contracts or have some characteristics of DeFi but do not meet all elements of a decentralized protocol. As part of this effort, Congress should consider codifying language expressing which portions, if any, of the DeFi

396 *Id.* at 14, 15.

397 *Id.* at 15 (emphasis omitted).

398 *Id.*

399 *See id.* at 15-16.

400 *See id.*

401 *See id.* at 14, 15, 18.

402 FinCEN, FIN-2014-R002, Application of FinCEN's Regulations to Virtual Currency Software Development and Certain Investment Activity (Jan. 30, 2014), https://www.fincen.gov/sites/default/files/administrative_ruling/FIN-2014-R002.pdf.

403 31 C.F.R. § 1022.210 (2024).

ecosystem should have AML/CFT obligations and the kinds of obligations actors should have by constructing the parameters of an AML/CFT framework appropriate to the class of activity.

Depending on the definition, this could include services that custody assets or have centralized governance, including through instances in which governance tokens are held by one or a small group of persons that can effectively assert control. In considering statutory changes, Congress should recognize the good practices that some participants in the DeFi ecosystem are implementing and focus on which entities are best positioned to mitigate illicit finance risk. Parts of the ecosystem, such as certain application layer participants, relayers, and remote procedure call (RPC) nodes, are currently implementing risk mitigation measures, including risk-rating wallets and rejecting transactions above a certain risk score. Subject to Congress's direction, Treasury could apply specified obligations to actors in the DeFi ecosystem based on the role that they play and the attendant risks.

Further Improvements to the AML/CFT Regime

In October 2023, FinCEN issued a notice of proposed rulemaking that proposed requiring financial institutions and financial agencies to implement certain recordkeeping and reporting requirements relating to transactions involving convertible virtual currency (CVC) mixing.[404] FinCEN received over 2,200 comments in response to the proposal. Concerns remain about how illicit actors, such as DPRK and ransomware actors, continue to use mixers to obfuscate and launder funds. Nevertheless, lawful users of digital assets may leverage mixers to enable financial privacy when transacting through public blockchains. To maintain the balance of those critical objectives, Treasury should consider the need to mitigate illicit finance risks, protect privacy, and reduce burden to the financial sector to evaluate appropriate next steps.

The United States has observed digital asset service providers and other actors attempting to avoid BSA obligations by domiciling in jurisdictions with weaker or non-existent regulatory frameworks or enforcement capacity, while still providing services that reach U.S. customers and even substantially impacting the U.S. digital asset ecosystem. This places U.S.-based industry actors at a disadvantage.

Recommendations

- Treasury should faithfully and expeditiously implement the Guiding and Establishing National Innovation for U.S. Stablecoins Act (GENIUS), which, among other things, requires Treasury to adopt rules to treat permitted payment stablecoin issuers as financial institutions under the BSA and to seek public comment and conduct research to identify innovative or novel methods, techniques, or strategies that regulated financial institutions use to detect illicit activity involving digital assets.[405]
- Digital asset market structure legislation should consider creating digital asset specific financial institution types or sub-types within the BSA. Now that GENIUS has been enacted into law, and pending additional market structure legislation being considered by Congress, 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.
- Legislation should consider specifying actors within the decentralized finance ecosystem that should have AML/CFT obligations, taking into consideration those actors' roles in the ecosystem and attendant risks.
- Treasury should consider next steps regarding its proposed rulemaking concerning CVC mixing.

404 *See* Proposal of Special Measure Regarding Convertible Virtual Currency Mixing, as a Class of Transactions of Primary Money Laundering Concern, 88 Fed. Reg. 72701 (Oct. 23, 2023).

405 S. 1582, 119th Cong. (2025) §§ 9(a)-(c) (enacted).

- 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.
- Congress should evaluate the self-custody language that is included in CLARITY[406] and codify the following principles through legislation that reinforce the importance of self-custody:[407]
  - *Principle 1*: The importance of U.S. individuals maintaining the capability to lawfully hold, or custody, their own digital assets without a financial intermediary.
  - *Principle 2*: The importance of enabling U.S. individuals to engage in lawful, direct digital asset transfers that do not involve a financial intermediary with another individual that lawfully self-custodies digital assets.
- Congress should codify principles regarding how control over an asset impacts BSA obligations, particularly for money transmitters, through legislation such as the Blockchain Regulatory Certainty Act,[408] which has been incorporated into CLARITY.
  - Specifically, such legislation could codify that a software provider that does not maintain total independent control over value is not engaged in money transmission for purposes of the BSA.[409]

Enhancing Effective Supervision

As the United States further develops a regulatory framework for digital assets and the number of supervised financial institutions in the digital asset ecosystem increases, it will be critical for relevant regulatory supervisors to enhance capabilities and expertise to supervise digital asset firms, as well as traditional financial institutions engaged with digital asset or digital asset actors.

Banks, credit unions, and other financial institutions interested in providing services to the digital asset industry or digital asset services to their customers may have questions about BSA obligations as they extend new services or develop new relationships.[410] Accordingly, supervisors administering and examining for BSA obligations should consider where additional guidance would enhance institutions' abilities to interact with digital assets and digital asset actors.

At present, experience with and resources devoted to supervision of digital assets firms varies across supervisory agencies. Ensuring effective and more consistent supervision and examination of digital asset service providers for AML/CFT requirements may require: (i) training; (ii) evaluating examination cycles and priorities based on risk; (iii) increasing the number of supervisors focusing on digital asset firms; and (iv) updating examination manuals to cover digital assets. Moreover, communication and information sharing on risks, best practices, and challenges across supervisors could support more effective supervision. Emphasis on effective, risk-based supervision should be central to these efforts, in contrast to a technical, one-size-fits all approach that does not make distinctions in risk profiles across supervised financial institutions. Effective supervision can reduce burdens for both supervisors and for financial institutions under their jurisdiction, allowing each to allocate resources in a manner consistent with risk. Moreover, this approach avoids placing unwarranted burden on lower-risk sectors, entities, and activities. Such efforts also present an opportunity to allow for more risk-based and effective supervision of financial institutions, including digital assets firms, in line with broader efforts to strengthen the U.S. AML/CFT framework.

406 H.R. 3633, 119th Cong. (2025)
407 Protecting these capabilities should not inhibit the ability or authority to carry out enforcement actions or special measures authorized under applicable law.
408 H.R. 3533, 119th Cong. (2025); *see* Emmer's Securities Clarity Act and Blockchain Regulatory Certainty Act, *supra* note 196.
409 *See* FinCEN, FIN-2019-G001, *supra* note 389, at 15, 18.
410 *See* Chapter IV.

Recommendations

- 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.
- Supervisors should evaluate whether additional compliance tools, training, and internal resources are needed to ensure examiners can effectively and efficiently evaluate institutions' digital asset-related policies, procedures, and programs.

Adapting BSA Reporting to Better Account for Digital Assets

A critical component of the BSA regime is the mandatory reporting intended to provide highly useful information for criminal, tax,[411] and regulatory investigations, risk assessments, or proceedings, as well as intelligence or counterintelligence activities to protect against terrorism.[412] These reports enable law enforcement and national security agencies to identify criminal activity, find otherwise opaque connections between related criminal actors, and locate assets derived from criminal activity that can be seized and, at times, returned to crime victims. While these reports are useful to law enforcement and national security agencies, creating and filing these reports imposes a burden on filers. As reporting obligations are considered, the burdens and benefits of reporting, as well as privacy concerns, must be carefully weighed.

Suspicious Activity Reports

Under the BSA and its implementing regulations, covered financial institutions are obligated to file Suspicious Activity Reports (SARs) when the institution knows, suspects, or has reason to suspect that a transaction conducted or attempted by, at, or through the financial institution (i) involves funds derived from illegal activity or is intended or conducted to disguise funds derived from illegal activity; (ii) is designed to evade any requirement of FinCEN's regulations or any other regulation promulgated under the BSA; (iii) lacks a business or apparent lawful purpose, or is not the sort in which the particular customer would normally engage and the financial institution knows of no reasonable explanation for the transaction; or, for some institutions, (iv) involves the use of a financial institution to facilitate criminal activity.[413]

Certain financial institutions, including digital asset service providers, have expressed that the SAR reporting regime could be more effective, both at providing key intelligence for law enforcement and national security agencies and ensuring financial institutions are directing their resources towards generating the most significant and impactful SARs.

As part of its efforts to implement the AML Act, Treasury is in the process of comprehensively reviewing its SAR regulations, guidance, and the SAR form itself, to maximize the value and efficiency of the reporting, while protecting individual privacy. As part of this process, Treasury should consider how best to update the form to facilitate inclusion of digital asset-specific information, which could increase the utility of these reports to law enforcement conducting digital assets-related investigations. Treasury should also consider how to streamline reporting for less complex reports and—as part of this review—consider how to enhance financial institutions' use of technology, including artificial intelligence and machine learning.

411 In addition to BSA reporting, the IRS uses reporting provided for Federal tax purposes to prevent tax evasion. For further discussion of current and proposed tax reporting regimes, *see* Chapter VII.

412 31 U.S.C. § 5311.

413 *See* 31 U.S.C. § 5218(g); *see also* 31 C.F.R. §§ 1020.320, 1021.320, 1022.320, 1023.320, 1024.320, 1025.320, 1026.320, 1029.320, 1030.320 (2024).

Recommendation

- Treasury should continue to evaluate modernizing Suspicious Activity Report (SAR) reporting, including the SAR form itself, to ensure it captures highly useful information.

Other BSA Forms

In addition to reporting by financial institutions, the BSA and its implementing regulations require other entities to file certain reports that provide highly useful information. For example, the BSA directs Treasury to require citizens of the United States, among others, to "keep records and file reports" when they maintain a relationship "with a foreign financial agency." Pursuant to this direction, Treasury requires each U.S. person having a financial interest in, or signature or other authority over, a bank, securities, or other financial account in a foreign country to file a Report of Foreign Bank and Financial Accounts (FBAR).[414] Although the FBAR does not currently require reporting related to digital assets, reporting required by FBAR regulations in some circumstances overlaps with reporting required by the Foreign Account Tax Compliance Act. Chapter VII contains more discussion and recommendations related to this reporting.

Additionally, the BSA, the Internal Revenue Code, and their respective implementing regulations require any person engaged in a trade or business who, in the course of such trade or business, receives more than $10,000 in coins or currency in one transaction or two or more related transactions to file a Form 8300 with FinCEN or the IRS.[415] In 2021, Congress amended the Internal Revenue Code to incorporate digital assets into the Form 8300;[416] however, digital asset transactions are not yet required to be reported as implementing regulations have not yet been made.[417] Chapter VII discusses how any IRS regulations implementing these rules would account for stakeholder concerns.

Although Congress amended the Internal Revenue Code, it did not amend the corresponding authority in the BSA. Once digital asset transactions are required to be reported on Form 8300, this discrepancy may create substantial industry confusion as trades and businesses may be required to follow one procedure if a reportable transaction involves digital assets and another if the reported transaction involves fiat currency.

Recommendation

- Congress should, through appropriate legislation, ensure that the information required by statute to be reported to FinCEN for BSA purposes under 31 U.S.C. § 5331 conforms with the information required to be reported by statute to the IRS for federal income tax purposes under 26 U.S.C. § 6050I, as was the case prior to 2021.

Improving Sanctions Compliance Regarding Digital Assets

OFAC sanctions regulations apply to all U.S. persons, including digital asset exchanges, technology companies, software developers, or other digital asset industry participants, that are subject to U.S. jurisdiction.[418]

414 31 C.F.R. § 1010.350 (2024).

415 31 U.S.C. § 5331; 26 U.S.C. § 6050I; 31 C.F.R. § 1010.330(a)(1)(ii) (2024). The $10,000 threshold for reporting transactions was established in 1984 (IRS) and 2001 (FinCEN) and has never been adjusted for inflation.

416 Note that the constitutionality of this amendment is currently being litigated. *See Carman v. Yellen*, No. 5:22-cv-00149 (E.D. Ky.).

417 Internal Revenue Service, IR-2024-12, Treasury and IRS Announce That Businesses Do Not Have to Report Certain Transactions Involving Digital Assets Until Regulations Are Issued (Jan. 16, 2024), https://www.irs.gov/newsroom/treasury-and-irs-announce-that-businesses-do-not-have-to-report-certain-transactions-involving-digital-assets-until-regulations-are-issued.

418 The key terms of each sanctions program are defined in the implementing regulations or Executive Orders, as appropriate. The term "U.S. persons" is defined in many implementing regulations to include "any United States citizen, permanent resident alien, entity organized under the laws of the United States or any jurisdiction within the United States (including foreign branches), or any person in the United States." Additionally, non-U.S. persons are also subject to certain OFAC prohibitions. For example, non-U.S. persons are prohibited from causing or conspiring to cause U.S. persons to wittingly or unwittingly violate U.S. sanctions, as well as engaging in conduct that evades U.S. sanctions.

Although OFAC may impose civil penalties for sanctions violations based on strict liability,[419] OFAC's sanctions compliance program expectations for digital assets industry participants are risk-based, not rigid or prescriptive.[420] Additionally, to promote clarity, innovation, and compliance with sanctions obligations, Treasury prioritizes engagement with the digital asset industry to educate participants on sanctions obligations, including through informal engagements and discussions as well as formal outreach at industry-focused conferences. OFAC uses these engagements to share existing industry guidance and public resources, such as OFAC's Compliance Hotline, which industry participants and the broader public can use to contact OFAC for guidance around sanctions regulations. These resources are key to ensuring that industry participants, including companies developing new offerings that may not understand how sanctions obligations apply, have access to OFAC guidance which they can rely on as they innovate in the digital assets sector.

Still, some digital asset firms have expressed a desire for additional resources explaining sanctions obligations related to various business models. Given that sanctions obligations apply to all U.S. persons and not just financial institutions or businesses, this is particularly relevant for developers who are creating software in the DeFi space. Developers and technologists should have clear resources available to them so that they understand how sanctions obligations apply. Based on feedback from the private sector, OFAC could consider publication of additional resources to further promote digital asset industry compliance with sanctions obligations.

Recommendations

- Treasury should issue a Request for Information (RFI) to directly solicit sanctions compliance information, input, and recommendations from industry participants to understand ongoing developments and innovations and gaps in existing OFAC guidance as well as to identify opportunities for enhanced private sector collaboration.
- Treasury should consider revising and updating OFAC's existing *Sanctions Compliance Guidance for the Virtual Currency Industry* brochure, which highlights existing compliance tools such as traditional sanctions screening and blockchain analytics to help improve sanctions compliance by all industry participants, in accordance with insight gleaned from the RFI process.

Advancing Privacy Through Digital Identity and Related Tools

The public nature of many blockchains provides insight into financial activities in digital assets, which can be used to support AML/CFT and sanctions compliance. While public blockchains provide certain transparency, some digital asset users may want to preserve their privacy when conducting transactions. The Working Group supports civil liberties protections surrounding privacy and the ability of individuals to privately transact on public blockchains. Enabling privacy is also critical to enabling the increased use of digital assets for payments as individuals may not want to publicly disclose every purchase of goods or services or allow salary payments or other private transactions to be tracked.

At the same time, regulated intermediaries need to be able to identify customers, report suspicious activities, and freeze or block certain transactions in line with their BSA and sanctions obligations. Several entities in the digital asset industry are developing tools designed to support various elements

419 Note that OFAC takes a number of factors into consideration when determining whether to assess a civil monetary penalty, and, if so, what penalty would be appropriate (e.g., willfulness, reckless, and knowledge of the conduct at issue, as set forth in OFAC's Economic Sanctions Enforcement Guidelines, 31 C.F.R. pt. 501, Appendix A (2024)).

420 OFAC has issued guidance specific to the digital asset to promote understanding of, and compliance with, sanctions requirements and due diligence best practices. *See generally* OFAC, Sanctions Compliance Guidance for the Virtual Currency Industry (Oct. 2021), https://ofac.treasury.gov/media/913571/download?inline.

of AML/CFT and sanctions compliance while maximizing user privacy. For example, digital identity technologies, identity proofing solutions, and other credentialing approaches can support regulated digital asset intermediaries in verifying identities of customers while preserving user privacy. Digital asset intermediaries could also use these tools as a safeguard against malicious actors attempting to gain unauthorized access to user accounts. While the applicability of these tools varies by operational models, governance, trustworthiness, and convenience, they offer a potential pathway to support intermediaries' risk mitigation in the digital asset ecosystem.

Some private sector digital identity tools combine online and offline components. For example, some digital credentials are issued based on physical attributes, such as requiring a credential recipient to appear in person or requiring physical documents for verification prior to issuance of a credential. Additionally, some tools may use unique capabilities within the digital asset space, with some tools tokenizing credentials and others tying the credential to a digital asset wallet address and preventing transfers to other addresses. These tools could potentially be used by regulated digital asset intermediaries to support onboarding or by a DeFi services' smart contracts to automatically check for a credential before executing a user's transaction. These tools could also potentially incorporate a user's transaction history on the public blockchain into their identity profile, providing additional information to digital asset intermediaries and other counterparties on a user's behavior and exposure to illicit finance risks.

To maximize privacy, some tools use Zero Knowledge Proofs,[421] which can enable users to confirm that their identity has been verified or subject to screening by a third party without revealing underlying personal information. Depending on the design of the tool, access to underlying personal information could be allowed at the user's request or with their permission. Additionally, some technologies allow selective disclosure of attributes, in which a user can decide which personal information to share with the recipient. These technologies can potentially support a path to enabling greater privacy preservation in customer identification models.

Further evolution of these tools, however, may require additional exploration on how private sector tools can adequately verify customers and protect their data. Regulatory bodies should provide additional clarity to financial institutions on how these tools can be used to identify and verify customers and to comply with other AML/CFT and sanctions obligations.

Moreover, digital identity solutions offer innovative capabilities to protect sensitive information and to reduce compliance burdens associated with verifying identifies. For example, the ability to pass a credential with only the necessary identifying information for a particular task both ensures that information is not unnecessarily exposed should an institution's systems be compromised and streamlines the verification process. As these solutions continue to mature, regulators should consider how to encourage the use of privacy-preserving technologies and ensure financial institutions can take advantage of their benefits, including by, where appropriate and consistent with risk, being able to rely on another financial institution's performance of customer identification.

421 A "zero-knowledge proof" is a "cryptographic scheme where a prover is able to convince a verifier that a statement is true, without providing any more information than that single bit (that is, that the statement is true rather than false)." *Glossary: Zero-Knowledge Proof*, National Institute of Standards and Technology, https://csrc.nist.gov/glossary/term/zero_knowledge_proof (last visited July 13, 2025).

Recommendations

- Treasury should consider coordinating with the National Institute of Standards and Technology (NIST), and other federal agency partners as appropriate, to:
  - Identify emerging approaches to implement customer identification in digital asset scenarios, including possible applications of the Fourth Revision of the NIST Digital Identity Guidelines (SP 800-63-4) to these scenarios.
  - Evaluate lessons learned in the project "Accelerate Adoption of Digital Identities on Mobile Devices" being executed in the National Cybersecurity Center of Excellence for applicability to customer identification programs in digital asset scenarios.
  - Evaluate the digital asset ecosystem, including existing identity credentialing tools and technical aspects of digital asset services, to determine potential approaches for defining, mandating, and enforcing customer identification programs and evaluate the potential efficacy of such schemes in detecting, deterring, and investigating fraudulent transactions.
- As is required by GENIUS, Treasury should issue an RFI to gather information on innovative tools to detect illicit activity, including with respect to digital identity verification.[422]
- Utilizing the information gathered from such RFI, additional research, and industry engagement, Treasury should, in consultation with the federal functional regulators,[423] consider issuing guidance to financial institutions on how they can utilize digital identity solutions within their existing customer identification programs.[424] Treasury should ensure that future guidance balances secure identity verifications with protection of personally identifiable information.

Equipping Digital Asset Actors to Mitigate Risk

Protecting the digital asset ecosystem from misuse requires strong partnership between the public and private sectors. The government relies on financial institutions to comply with AML/CFT and sanctions obligations designed to identify, report, and mitigate illicit finance risks. As such, it is critical that the private sector is equipped with the appropriate authorities and a strong understanding of risk to combat misuse.

Enabling Private Sector Investigations

Some characteristics of digital assets, including the ability to rapidly transfer digital assets across borders, can present challenges in identifying and disrupting illicit activity involving these assets. Moreover, digital asset transfers are typically irreversible, further reducing the likelihood that funds, even if quickly reported, can be recovered. To mitigate this risk, some digital asset institutions, including exchanges and stablecoin issuers, may in some circumstances wish to temporarily hold assets when they identify suspected illicit activity. During the time those assets are held, institutions can investigate and determine whether, for example, the asset is stolen or linked to fraud or other criminal activity. Enabling institutions to identify and temporarily hold property involved in suspected illegal activity will equip these institutions with ability to control risk and protect digital asset users.

At times, however, institutions may feel constrained in their ability to temporarily hold assets to investigate suspected illegal activity. In other contexts, some states have enacted digital asset specific-"hold laws" that

422 S. 1582, 119th Cong. (2025) § 9(a) (enacted).

423 "Federal functional regulators" means the SEC, CFTC, FDIC, OCC, FRB, and NCUA. 31 U.S.C. § 5318.

424 *See* S. 1582, 119th Cong. (2025) § 9(d) (enacted).

offer safe harbors to institutions that temporarily hold property involved in suspected illegal activity during the pendency of a short duration investigation.[425] The ability to temporary hold property as authorized by such laws enable institutions to, for example, contact a user to ascertain whether they are a scam victim or whether an asset has been stolen.

Recommendation

- Congress should consider enacting a digital asset-specific "hold law" that offers a safe harbor to institutions that temporarily and voluntarily hold property involved in suspected illegal activity during a short duration investigation. Such a law should consider transparency when an asset is frozen and consumer protection measures.

Increasing Public-Private Cooperation

Public-private partnerships play a critical role in sharing trend and operational information to support actions to deter and disrupt illicit activity. For example, the private sector has insight into emerging risks, challenges in complying with AML/CFT and sanctions obligations, and innovative measures to mitigate these risks. The Working Group supports efforts across the Federal government to solicit private sector input when evaluating potential policy directions or developing guidance and regulations.

Treasury, to highlight one example of these efforts, held private sector roundtables in May 2025 to discuss DeFi, stablecoins, and cybersecurity. During the roundtables, more than thirty industry participants shared good practices, challenges, and recommendations for how the Federal government can promote responsible innovation in the digital asset ecosystem. Building on the May roundtables, in July 2025 FinCEN held a FinCEN Exchange[426] to convene traditional financial institutions, digital asset service providers, compliance tool providers, industry associations, and law enforcement to discuss responsible innovation, industry challenges, new compliance tools, compliance best practices, and fraud and scam typologies. Treasury will continue engaging with the private sector through similar forums and bilateral meetings to both share information and to learn from industry about developments in the digital asset ecosystem. This can include further engagements to discuss innovative compliance tools and good practices employed by DeFi participants, such as application layer participants (front ends), relayers, and RPC nodes, to mitigate illicit finance risks. Moreover, the Federal government shares trends on illicit finance risks in digital assets through products like FinCEN alerts or advisories, FBI's Public Service Announcements, and public-private partnership efforts, including FinCEN Exchange as well as direct engagement.

The Federal government also enables sharing actionable information, including through FinCEN's 314(a) and 314(b)[427] programs and the Illicit Virtual Asset Notification (IVAN) public-private partnership. Through the 314(a) program, law enforcement authorities can submit identifiers to financial institutions about individuals, entities, and organizations engaged in or reasonably suspected, based on credible evidence, of engaging in terrorist acts or money laundering activities. Upon receiving the identifier, a financial institution confirms whether it has additional information on the entity.[428] The complementary 314(b) program provides financial institutions with the ability to share information with one another, under a safe harbor that offers protections

425 *See generally* American Bankers Association Foundation, State "Hold" Laws and Elder Financial Exploitation Prevention: A Survey Report (2025), https://www.aba.com/-/media/documents/reference-and-guides/2025-sbfs-elder-law-survey-report.pdf?rev=a5327479843f4d4c9b1366c7ef43ddfa.

426 FinCEN Exchange is a voluntary public-private information sharing partnership among FinCEN, law enforcement agencies, national security agencies, financial institutions, and other private sector entities to enhance coordination, communication, and feedback in the fight against financial crimes. Launched in 2017, FinCEN Exchange was designed to enable financial institutions to better identify and report information on the highest priority illicit finance risks to the U.S. financial system and national security. Congress statutorily established FinCEN Exchange through Section 6103 of the Anti-Money Laundering Act of 2020, codified at 31 U.S.C. § 310(d).

427 References to "314" are derived from the programs' statutory authority, Section 314 of the USA PATRIOT Act. Regulations implementing Section 314 are codified at 31 C.F.R. § 1010.520 (implementing Section 314(a)) and § 1010.540 (implementing Section 314(b)) (2024).

428 *See* 31 C.F.R. § 1010.520(b) (2024).

from liability, in order to better identify and report activities that may involve money laundering or terrorist activities.[429] IVAN is a public-private partnership platform through which partners can share information associated with the utilization of digital assets in support of illicit activity, along with identification and mitigation of said threats. IVAN enables participants to root out nefarious actors hoping to hide behind virtual assets and the underlying blockchain technology.

Given the characteristics of digital assets noted above, it is critical that the public and private sectors can quickly share information about illicit finance risks. The Working Group supports this information sharing—provided it is used for the purpose prescribed in the law to target illicit finance and terrorist activity—to more effectively target bad actors operating in the digital asset ecosystem. It is imperative that this information sharing not be used to infringe on the civil liberties of law-abiding citizens and such digital assets users. Wide and meaningful participation in IVAN and the 314(a) and 314(b) programs could increase both the amount of information shared as well as the firms that are able to act upon the information, potentially making the digital asset ecosystem safer and protecting U.S. users.

Recommendations

- Treasury should undertake efforts to encourage greater information sharing, including through FinCEN's 314(a) and 314(b) programs. Such efforts should include encouraging domestic and cross-border information sharing, greater participation in sharing programs by digital asset financial institutions and improved information sharing between digital asset and traditional financial institutions.
- Public and private sector participation in real-time information sharing through IVAN should be encouraged to the extent consistent with legal obligations.

Disrupting and Mitigating Systemic Illicit Finance Risks

The Federal government takes a whole of government approach to disrupting and exposing illicit activity in the digital asset ecosystem. This approach and use of authorities prevents bad actors from using digital assets to facilitate money laundering and illicit activity, deprives bad actors of their proceeds, and, when possible, compensates victims. These efforts make the digital asset ecosystem safer for U.S. digital asset users and service providers while also promoting U.S. national security.

The Federal government uses OFAC sanctions and FinCEN authorities to counter foreign actors, like DPRK or ransomware cybercriminals, and their facilitators, including foreign digital asset service providers that enable illicit activity and are not subject to the clear requirements under OFAC and FinCEN regulations in the United States. Additionally, when necessary, the Federal government uses civil enforcement actions to impose consequences on firms operating without taking appropriate steps to mitigate illicit finance risks in violation of applicable laws and regulations. Both FinCEN and OFAC have taken several civil enforcement actions for violations of their applicable laws and regulations that have exposed illicit actors, addressed the abuse of digital assets, and driven compliance with regulatory obligations.

Law enforcement also plays a critical role in this effort through seizures, takedowns, and criminal prosecution to support these objectives. In particular, law enforcement seizure and forfeiture capabilities are critical to support the compensation of victims for losses in digital assets and for losses converted by criminals into digital assets.

However, as described below, there are some limitations on how the Federal government can effectively use these tools to support these objectives. For example, Treasury's authorities are not always clearly applicable

429 *See* 31 C.F.R. § 1010.540(b) (2024); *see also* FinCEN, Section 314(b) Fact Sheet (Dec. 2020), https://www.fincen.gov/sites/default/files/shared/314bfactsheet.pdf.

in the digital asset space, and law enforcement's authorities should be updated to better address abuse in the digital assets ecosystem and better compensate victims.

Applying Treasury Authorities to Digital Asset Ecosystem

As noted above, FinCEN and OFAC use authorities to disrupt and expose foreign illicit activity in the digital asset ecosystem, focusing on key means used by malicious actors to profit from their crimes. However, some existing tools and authorities are not always applicable to or as effective in the digital asset ecosystem. As explained below, certain FinCEN authorities restrict or prohibit U.S. financial institutions from establishing or maintaining correspondent or payable-through accounts for foreign financial institutions facilitating illicit financial activity, but those authorities are less impactful when digital asset exchanges are not reliant on correspondent relationships.

Tailoring Section 311 Authorities for Digital Assets

Section 311 of the USA PATRIOT Act authorizes the Secretary of the Treasury to identify a foreign jurisdiction, foreign financial institution, class of transactions, or type of account as being a "primary money laundering concern," and to require domestic financial institutions and domestic financial agencies to take one or more of five "special measures."[430] The five special measures are prophylactic safeguards that defend the U.S. financial system from money laundering and terrorist financing. The Secretary of the Treasury has delegated authority to administer the BSA, including but not limited to Section 311, to the Director of FinCEN.[431] FinCEN may therefore impose one or more of these special measures to protect the U.S. financial system from these threats. Special measures one through four impose additional recordkeeping, information collection, and reporting requirements on covered U.S. financial institutions.[432] The fifth special measure allows FinCEN to prohibit, or impose conditions on, the opening or maintaining in the United States of correspondent or payable-through account for or on behalf of the identified primary money laundering concern.[433] These special measures under Section 311 frequently require notice and comment rulemaking.[434]

FinCEN has encountered limitations when applying its Section 311 authority to digital assets. Specifically, the fifth special measure is limited to correspondent or payable-through accounts, which do not translate to the digital asset industry.

Congress has given FinCEN newer authorities, similar to Section 311, in Section 2313a of the Fentanyl Sanctions Act[435] and Section 9714 of the Combating Russian Money Laundering Act[436] to address primary money laundering concerns in connection to illicit opioid trafficking and Russian illicit finance, respectively. The new authorities are limited to specific areas of money laundering concern but allow FinCEN to prohibit, or impose conditions upon, certain transmittals of funds, as defined by the Secretary of the Treasury, by any domestic financial institution or domestic financial agency. By using "certain transmittals of funds" instead of "correspondent or payable-through accounts," the new authorities can be applied to both traditional finance and digital assets.

430 Section 311 of the Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT) Act of 2001 (codified at 31 U.S.C. § 5318A).

431 U.S. Department of the Treasury, Treasury Order 180-01 (Jan. 14, 2020), https://home.treasury.gov/about/general-information/orders-and-directives/treasury-order-180-01.

432 *See* 31 U.S.C. § 5318A (b)(1) - (b)(4).

433 31 U.S.C. § 5318A(b)(5).

434 31 U.S.C. § 5318A(a)(3).

435 *See* 21 U.S.C. § 2313a.

436 Section 9714 (as amended) can be found in a note to 31 U.S.C. § 5318A.

Recommendation

- Congress should, consistent with how it has approached Fentanyl and Russian illicit finance, add a sixth special measure to Section 311 authorizing FinCEN to prohibit, or impose conditions upon, certain "transmittals of funds" that are not tied to a correspondent banking relationship. This would enable Treasury to target foreign digital asset exchanges or digital asset transactions involving criminal or state actors—without regard to the nature of their illicit activity.

Leveraging OFAC Authorities to Disrupt Malicious Foreign Digital Asset Actors

OFAC continues to use its sanctions authorities to target the illicit use of digital assets, especially instances in which digital assets are used in conjunction with (i) crimes targeting Americans, (ii) laundering proceeds of illicit drug and narcotics sales, and (iii) terrorist organizations or the Iranian regime. Since January 2025, OFAC has added dozens of digital asset wallet addresses and other identifiers to the sanctions list across multiple sanctions programs in support of U.S. national security priorities to constrain foreign criminal and state actor abilities to generate and move illicit funds. OFAC is also exploring how calibrated uses of its authorities could strengthen its ability to force foreign digital asset firms and users to choose between accessing the U.S. market, or providing financial support to sanctioned drug traffickers, weapons proliferators, and terrorist financiers.

Recommendation

- Treasury should continue to use OFAC's sanctions authorities, which range from applying full blocking sanctions to more calibrated restrictions, to target malicious actors seeking to harm Americans and to limit the access of foreign digital asset actors engaged in illicit activity to U.S. markets, in support of the Trump Administration's priorities.

Tailoring Law Enforcement Capabilities and Authorities

Criminal actors who victimize Americans and exploit the legitimate financial sector harm the U.S. economy and interfere with the responsible use and growth of digital assets. Holding these criminal actors accountable supports the Trump Administration's policies, including by targeting the financial networks that enable transnational criminal organizations to profit, protecting victims, and promoting U.S. leadership in digital assets. Enhancing the authorities of the DOJ and U.S. federal law enforcement agencies will strengthen the United States' ability to achieve these goals.

Improving Crime Victim Compensation Regulations

The Asset Forfeiture Program is essential to the fight against transnational criminal organizations, including cartels, that perpetuate violence, drug trafficking, human trafficking, and drive the opioid crisis. Prosecutors have used asset forfeiture robustly to recover digital assets involved in fraud or theft, sometimes involving assets worth significant amounts. The asset forfeiture statutes, in addition to providing powerful tools to deny criminals the proceeds of crime and disrupt criminal organizations, provide discretion to use forfeited assets to compensate victims. Accordingly, the DOJ uses its authorities to provide discretionary victim compensation through the Department's Asset Forfeiture Program, but the regulations governing the remission and mitigation of forfeitures have not been amended since 2012. Since that time, the Asset Forfeiture Program has grown significantly, and forfeiture has also become an essential tool to fight fraud and other financial crime, including digital asset-related thefts and scams. As a result, certain aspects of the remission regulation need revision to enhance victims' recoveries. Current regulations governing the use of forfeited funds to compensate victims, 28 C.F.R. Part 9, can be updated to increase compensation and simplify procedures for victims of crime, including digital asset-related fraud and theft, and to increase government efficiency.

Revisions to these regulations would allow greater victim compensation, more like that available through criminal restitution, and simplify procedures for compensating victims and returning property to innocent owners.

Enhancing Criminal Laws to Protect Investigations and Penalize Bad Actors Targeting Digital Assets

Protecting the digital asset ecosystem requires that prosecutors have the necessary authorities to counter bad actors who seek to exploit it. Statutes authorizing criminal charges and sentencing guidelines could be amended to ensure that bad actors who misuse digital assets or victimize digital asset owners or investors are appropriately charged and sufficiently penalized, and to ensure that prosecutors can appropriately recover those assets.

Address Gaps in Criminalizing False Statements to Financial Institutions

Transnational criminal organizations, cartels, terrorists, and other criminals need access to the U.S. financial system to move the money and digital assets that fuel their crimes. These criminals often make fraudulent or false statements to financial institutions to obtain or maintain access to financial accounts and services so they can quickly move their ill-gotten gains. Existing law criminalizes certain fraud and false statements made to some kinds of financial institutions, as defined in Title 18 of the U.S. Code.[437] But because the law criminalizes only *certain* false statements to *certain* financial institutions, gaps exist—and criminal actors are actively exploiting them. First, the definition of "financial institution" in Title 18 of the U.S. Code is narrower than the definition in Title 31 of the U.S. Code, and thus omits virtual asset service providers.[438] In addition, the law does not apply to all false statements in connection with opening and maintaining access to services from financial institutions. Addressing these gaps would enable prosecution of more of the criminal misuse of digital assets by (i) making clear that lying to financial institutions to open or maintain accounts, including accounts used to launder digital assets and convert them into fiat currency, is a crime; and (ii) protecting all financial institutions, including those offering digital asset services, that are the target of criminal schemes.

Facilitate Criminal Investigations and Prosecutions for Digital Asset Theft

As digital assets continue to become more commonly held and stolen forms of property, it is important to use all appropriate charges to prosecute those who steal and transfer illicitly obtained digital assets. The National Stolen Property Act (NSPA) has served as an effective tool to prosecute those involved in the theft and subsequent interstate movement or transfer of traditional forms of property, including money and securities. But the statute does not explicitly include digital assets. Clarifying that digital assets are covered property for purposes of the NSPA would allow law enforcement to use this provision in appropriate criminal investigations and prosecutions.

Protecting Investigations and Enhancing Civil Remedies

Protect Investigations through Anti-Tip-Off Amendments

Tracing illicit proceeds through financial institutions is a complex and sensitive operation, made even more complicated when proceeds are converted to digital assets and moved across the ecosystem. If suspects are tipped off during the process, they can quickly move their assets and flee the United States. The anti-tip-off statute, 18 U.S.C. § 1510, prevents employees of financial institutions from tipping off their customers to ongoing investigations of certain violations. Without these protections, financial institutions may be subject to contractual or other requirements that could result in notification of sensitive ongoing investigations, impeding law enforcement. Some virtual asset service providers have argued that they are not financial institutions for

437 18 U.S.C. § 1014.

438 *Compare* 18 U.S.C. § 20 *with* 31 U.S.C. §§ 5312(a)(2) and (c).

the purpose of this statute. This can result in investigators limiting their efforts to pursue and recover illicit financial schemes involving digital assets or risk exposure of the investigation. To close this gap, the anti-tip off statute can be amended to cover all Title 31-defined financial institutions along with the current, more limited Title 18-defined financial institutions. Additionally, expanding the statute's list of covered offenses would close another gap in the law. Specifically, including serious underlying offenses, such as drug and human trafficking offenses, as covered offenses would prohibit agents of financial institutions from tipping off suspects about investigations targeting that conduct alongside other prohibited offenses.

Extending the Modified Tracing Requirement for Civil Forfeiture to Digital Assets

18 U.S.C. § 984 allows the Federal government to initiate civil forfeiture proceedings against certain property, including funds deposited in an account in a financial institution and cash "found in the same place or account" in the same amount that the government can trace to the illegal activity during the year before filing a civil complaint. This means that the government is not required to trace particular dollars by unique serial numbers to the illegal activity. This provision is particularly useful in cases where criminal proceeds are commingled with other funds. For example, if the government demonstrates that $50,000 in cash drug proceeds was deposited into an account that also contains other deposited funds, the statute authorizes the government to forfeit $50,000 from the account without showing that the forfeited funds are the exact same $50,000 in drug proceeds. The statute does not, however, apply to digital assets. Therefore, in a drug case in which a bad actor accepts payment in bitcoin and holds the bitcoin in a wallet that also contains other bitcoin, under current law, the government cannot forfeit the drug proceeds unless it can specifically trace particular bitcoin to the drug transaction.

Amending Section 984 to make certain digital assets subject to the same modified traceability requirement as exists for cash would allow the government to seize and forfeit digital assets found in the same wallet used to hold crime-linked digital assets, without requiring the government to prove the forfeited assets were the exact same digital assets derived from or used to commit a criminal offense.

Recommendations

- Congress should evaluate victim compensation regulations and propose amendments to address concerns regarding victim compensation and improve asset-forfeiture efforts in the digital assets space.[439]
- Congress should tailor 18 U.S.C. § 1014 to protect all financial institutions (defined under Title 31 of the U.S. Code), including those offering digital asset services. In addition, Congress should clarify that the law applies to all false statements in connection with obtaining or maintaining access to services from financial institutions. Relatedly, U.S.S.G. Section 2B1.1 should be updated to include a sentencing enhancement for making false statements to financial institutions where the scheme involves significant volume of criminal funds but no loss to the institution.
- Congress should amend the NSPA to clarify that digital assets are property subject to this act.
- Congress should amend the anti-tip-off provision in 18 U.S.C. § 1510 to update the definition of "financial institution" from the narrower definition found in 18 U.S.C. § 20 to the broader definition found in the BSA, 31 U.S.C. §§ 5312(a)(2) and (c), to cover, among other additions, certain digital asset firms that operate as money services businesses (MSBs). Congress should also amend the same anti-tip-off provision to include additional serious underlying offenses as covered offenses to prohibit agents of financial institutions from tipping off suspects.
- Congress should amend 18 U.S.C. § 984 to make certain digital assets subject to the same modified traceability requirement as exists for cash to allow the government to seize and forfeit digital assets found in the same wallet used to hold crime-linked digital assets, without requiring the government to prove the forfeited assets were the exact same digital assets derived from or used to commit a criminal offense.

439 *See* DOJ, Memorandum from the Deputy Attorney General, *supra* note 370, at 3. The DOJ has already begun these efforts.

Protecting the Digital Asset Industry from Malicious Cyber Actors

Strong cybersecurity practices are needed to safeguard digital assets from theft, fraud, and cyberattacks. The documented efforts of nation-state cyber groups and other illicit actors to steal or fraudulently acquire digital assets present a national security concern. DPRK has been particularly adept at stealing digital assets from market participants, illustrated by the theft of $1.5 billion from a digital asset firm in February 2025. DPRK uses complex social engineering schemes to compromise networks, posing a persistent threat to organizations with access to large quantities of digital assets or products. Critically, the Federal government assesses that DPRK uses digital assets to fund its weapons of mass destruction and ballistic missile programs. These hacks and the risks to U.S. digital asset users and national security demonstrate the need to improve cybersecurity measures within the digital asset industry.

This section discusses some of the cybersecurity challenges that the digital asset ecosystem faces and identifies measures that can be implemented to bolster cybersecurity. Malicious cyber actors exploit vulnerabilities in software, hardware protocols, or even human processes to penetrate a victim's security controls to maliciously alter code or conduct unauthorized transactions. To discover and exploit these vulnerabilities, malicious cyber actors conduct network scanning and reconnaissance. The availability of vulnerabilities may be exacerbated by the lack of cybersecurity requirements or audits in the digital asset space. Additionally, while there are several efforts to share threat information within industry and between the public and private sectors, information sharing could be further improved to strengthen industry's ability to defend against threats. Treasury, through its Office of Cybersecurity and Critical Infrastructure Protection (OCCIP), is currently exploring how to expand existing mechanisms to share cybersecurity-related information with the digital asset industry. The below explores some risks present in three segments of the digital asset industry designed to illustrate how malicious cyber actors exploit digital asset participants: custody services, smart contracts, and blockchain network validation processes. This is not, however, an exhaustive list.

OCCIP works to strengthen the security and resilience of financial services sector critical infrastructure and reduce operational risk. The office works closely with financial sector companies, industry groups, and government partners to share information about cybersecurity and physical threats and vulnerabilities. OCCIP's information sharing is primarily centered around traditional financial institutions but is exploring how to expand its efforts to digital asset firms. One example of its information sharing initiatives is Treasury's Automated Threat Information Feed (ATIF), which provides participants with access to a tailored cyber threat feed. The ATIF aggregates indicators from Treasury, open-source data feeds, Federal government partners, international partners, and participating members. The feed is available through Cloudflare to their existing customers, or through the Malware Information Sharing Platform, an open-source threat intelligence platform.

Additionally, Treasury chairs the Financial and Banking Information Infrastructure Committee (FBIIC), which is chartered under the President's Working Group on Financial Markets and is charged with coordinating efforts to improve the reliability and security of financial information infrastructure. OCCIP, as the delegated chair and the Secretariat of FBIIC, utilizes FBIIC for improving coordination and communication among financial regulators, enhancing the resiliency of the financial sector, and promoting public-private partnership.

Recommendations

- As noted in Chapter III, the Working Group recommends that relevant agencies develop principles-based requirements and standards, as appropriate, for digital asset firms. Such principles-based requirements and standards should take into account the various activities and related risks of various industry participants to strengthen industry's protection from malicious cyber actors.
- The Working Group recommends that relevant agencies consider measures to increase information sharing on potential threats across the private sector and between the public and private sectors.
- Treasury's OCCIP could work with industry to identify opportunities to increase information sharing on cybersecurity risks, including by providing U.S. regulated digital asset firms access to the ATIF.
- Treasury's OCCIP—through the existing public-private partnership structure—could explore identifying gaps in addressing operational resiliency of digital asset firms to enable broader adoption.

Custody: Digital asset firms that custody digital assets for retail or institutional customers can be attractive to illicit actors because of the large amount of funds that they hold. Attackers use a variety of techniques—phishing, often leveraging emailing and short message service (SMS); key logging; or social engineering—to illicitly gain access to a digital asset firm's custody infrastructure, either controlled by the firm or managed by a third-party provider. In some instances, this can include malicious cyber actors gaining access to the private keys to the firm's wallet addresses or exploiting other security gaps. Attackers can use access to steal funds from digital asset firms, potentially resulting in substantial losses. While digital asset firms that take custody of user assets are frequent targets, other digital asset participants that aggregate funds, including cross-chain bridges and unhosted wallet addresses with a large amount of digital assets, may also be attractive targets for malicious cyber actors.

Example Mitigation Measures

Digital asset firms custodying assets could:

- Implement policies and procedures designed to protect the confidentiality, integrity, and availability of information systems. These should be informed by a risk assessment and cover, among other topics, asset inventory and device management, data controls and identity management, and systems and network monitoring.
- Implement policies and procedures to define and limit user access privileges for digital asset operations and transaction processes. This should include policies for secure key management practices, specifically for signing keys, and ensuring that third party service providers, if applicable, have a solid track record of secure key management practices before using their services.
- Use tools to simulate and validate transactions prior to signing to confirm the intent of the transaction matches the outcome.
- Use digital identity tools to protect private keys and digital assets accounts.
- Enforce credential requirements and multifactor authentication (MFA). North Korean malicious cyber actors continuously target user credentials, email, social media, and private business accounts. Organizations should be aware of MFA interception techniques for some MFA implementations and monitor for anomalous logins and require users to change passwords regularly to reduce the impact of password spraying and other brute force techniques. The

Working Group recommends organizations implement and enforce MFA to reduce the risk of credential theft.

Smart Contracts: Smart contracts are programs on blockchain networks that automatically execute the terms of an agreement when specific conditions are met. Malicious actors can exploit unpatched vulnerabilities in smart contracts to their advantage. Not every bug will result in a catastrophic failure or allow for exploitation, and bugs often go unnoticed for years. While the ability to view open-source code for DeFi services' smart contracts may enable security engineers to review code for potential exploits, no software is immune to defects in code, regardless of whether it is open- or closed-source or used by one person or millions of entities worldwide. Coding flaws can be exploited by malicious cyber actors to remove funds from DeFi services without authorization, so it is essential to prioritize the security and quality of code on an ongoing basis. These risks may be exacerbated for smart contracts that lack a mechanism for alterations if a critical vulnerability is discovered or exploited.

Example Mitigation Measures

- Adhere to secure development practices, conduct quality assurance and control of smart contracts prior to deployment, and employ third-party auditing to reduce risk of software defects.
- Leverage trusted code libraries.
- Monitor for new vulnerabilities.
- Consider emergency stops and circuit breakers for unexpected smart contract issues.

CHAPTER VII

Taxation

Taxation

> The nature of Bitcoin is such that once version 0.1 was released, the core design was set in stone for the rest of its lifetime. Because of that, I wanted to design it to support every possible transaction type I could think of . . . . The design supports a tremendous variety of possible transaction types that I designed years ago. Escrow transactions, bonded contracts, third party arbitration, multi-party signature, etc. If Bitcoin catches on in a big way, these are things we'll want to explore in the future, but they all had to be designed at the beginning to make sure they would be possible later.
>
> **BitcoinTalk Forum Post Re: "Transaction and Scripts"**
> Satoshi Nakamoto, June 2010[440]

The advent and growth of digital assets has raised numerous questions about the application of federal income tax laws. The "tremendous variety of possible transaction types" Satoshi Nakamoto identified for digital assets—some of which have no analog in traditional assets—can make applying current provisions to digital asset transactions challenging. As such, providing guidance or enacting legislation that addresses the special characteristics of these digital assets and transactions will help taxpayers understand their federal tax obligations, and in turn promote the growth and use of digital assets in the United States.

Addressing aspects of federal tax law contrary to the goals of the Executive Order has been a priority since the first days of the Trump Administration. H.J. Res. 25, a joint resolution sponsored by Senator Ted Cruz and Representative Mike Carey, was signed into law by President Trump in April 2025.[441] This resolution overturned a Biden Administration effort to define certain DeFi developers as "brokers" for tax purposes, even though neither those developers nor their software ever held custody of their users' digital assets.[442] The Working Group applauds this action as an example of the pro-innovation approach to tax law the Federal government should embrace.

As background, federal tax law consists of the Internal Revenue Code (Code),[443] regulations implementing the Code, related statutes, tax treaties, and an extensive body of case law and associated common law doctrines that provide a foundation for statutory law and remain essential to interpreting it. The IRS also publishes Revenue Rulings and Notices providing its interpretation of the law to particular facts, which are not binding for taxpayers but generally relied upon.[444]

Crucial questions of federal tax law with respect to income derived from digital assets include evaluating timing, source, and character (i.e., capital income or ordinary income) and the appropriate application of statutory provisions. The guidance issued to date by Treasury and the IRS is described below.

---

440 satoshi, Comment to *Re: Transactions and Scripts: DUP HASH160 . . . EQUALVERIFY CHECKSIG*, BitcoinTalk (June 17, 2010 at 6:46 PM), https://bitcointalk.org/index.php?topic=195.msg1611#msg1611.

441 Pub. L. No. 119-5, 139 Stat. 48 (2025).

442 Press Release, Sen. Cruz Applauds Signing of Cryptocurrency Resolution into Law (Apr. 11, 2025), https://www.cruz.senate.gov/newsroom/press-releases/sen-cruz-applauds-signing-of-cryptocurrency-resolution-into-law; *see* Gross Proceeds Reporting by Brokers That Regularly Provide Services Effectuating Digital Asset Sale, 89 Fed. Reg. 106928 (Dec. 30, 2024) (no longer of force or effect).

443 Unless otherwise specified, all "Section" or "§" references in this tax chapter are to sections of the Code or the regulations issued thereunder.

444 A Revenue Ruling is an official interpretation by the Internal Revenue Service (IRS) of the Code, related statutes, tax treaties and regulations on how the law is applied to a specific set of facts and is published in the Internal Revenue Bulletin. A Notice is a public pronouncement that may contain guidance that involves substantive interpretations of the Code or other provisions of the law and is also published in the Internal Revenue Bulletin. Treas. Reg. § 601.601(d)(2)(i)(a) (2024); *Understanding IRS Guidance: A Brief Primer*, IRS, https://www.irs.gov/newsroom/understanding-irs-guidance-a-brief-primer (last visited July 13, 2025).

Current Tax Guidance on Digital Assets

Treasury and the IRS have issued regulations and related guidance addressing how digital assets are taxed ("substantive guidance") and relating to reporting on digital asset transactions by brokers and other intermediaries ("third-party information reporting").

Notice 2014-21 provides core guidance for digital asset transactions.[445] It provides that digital assets are treated as property, as opposed to currency, for federal income tax purposes, and that general federal income tax principles apply to digital asset transactions.[446] The Notice also provides FAQs addressing several specific issues as well. Other substantive guidance consists in part of published sub-regulatory guidance addressing hard forks,[447] staking,[448] and non-fungible tokens (NFTs).[449]

Treasury has proposed regulations relating to the corporate alternative minimum tax (CAMT) that do not reference digital assets but would affect how they are taxed. CAMT was signed into law by the Biden Administration as part of the Inflation Reduction Act of 2022.[450] A prior version of the CAMT was repealed, by President Trump, by the Tax Cuts and Jobs Act of 2017.[451]The impetus—at the time—to implement CAMT was to address differences between book income and taxable income, and CAMT sought to do so by creating a minimum tax on book income.[452] This policy is problematic for a multitude of reasons; most acutely, it attempts to combine two separate policy matters (financial accounting treatment versus tax treatment). Moreover, implementing a minimum tax on book income has the potential net effect of burdening investment. In fact, the Treasury Inspector General for Tax Administration, during the Biden Administration, found that "CAMT is a complex tax law" and that "IRS employees … have spent approximately 21,237 hours on the first six CAMT notice publication projects."[453] Further, given the complexities of the law, the "IRS waived failure to pay estimated tax penalties with respect to CAMT obligations in Tax Year 2023."[454] Needless to say, although CAMT does not specifically target the digital asset sector, it creates a potential punitive effect on the sector's growth, much like it could have an adverse impact on other sectors like oil and gas extraction. CAMT therefore contradicts the policy goals of Executive Order No. 14219, which directs agencies to identify and remove certain regulations and other guidance that among other things, impede private enterprise and entrepreneurship.[455]

Treasury and the IRS have published final regulations with respect to third-party information reporting implementing legislation that requires centralized brokers and other persons who take possession of customer

445 2014-16 I.R.B. 938 (Apr. 14, 2014). The Infrastructure and Investment Jobs Act, Pub. L. No. 117-58, 135 Stat. 429 (2021) amended the Code to define a digital asset, for purposes of information reporting by brokers, as any digital representation of value which is recorded on a cryptographically secured distributed ledger or any similar technology as specified by the Secretary. Notice 2014-21 referred to "convertible virtual currency." The term "digital asset" includes property that Treasury and the IRS have previously referred to as convertible virtual currency.

446 IRS, Notice 2014-21, *supra* note 445. Note that Notice 2023-34, 2023-19 I.R.B. 837 (May 8, 2023) modifies Notice 2014-21 but does not change its conclusions.

447 IRS, Revenue Ruling 2019-24, 2019-44 I.R.B. 1004 (Oct. 28, 2019).

448 IRS, Revenue Ruling 2023-14, 2023-33 I.R.B. 484 (Aug. 14, 2023).

449 IRS, Notice 2023-27, 2023-15 I.R.B. 634 (Apr. 10, 2023).

450 Pub. L. No. 117-169, 136 Stat. 1818 (2022).

451 Pub. L. No. 115-97, 131 Stat. 2054 (2017).

452 Book income refers to the amount of income corporations report on their financial statements based on applicable financial accounting standards, with material differences as compared to taxable income. This includes different treatment of losses, timing differences for when or whether income is recognized, and different treatment of costs and expenses (e.g., capitalization or deduction).

453 Treasury Inspector General for Tax Administration, Review of the Corporate Alternative Minimum Tax Implementation Identified Weaknesses in the Pre-Rulemaking Process (Sept. 9, 2024), https://www.tigta.gov/sites/default/files/reports/2024-09/2024308036fr.pdf.

454 *Id* at 4. The IRS has subsequently waived failure to pay estimated tax penalties with respect to CAMT obligations for tax years 2024 and 2025. *See* IRS, Notice 2024-33, 2024-18 I.R.B. 959 (Apr. 29, 2024); IRS, Notice 2024-47, 2024-27 I.R.B. 1 (July 1, 2024); IRS, Notice 2024-66, 2024-40 I.R.B. 682 (Sept. 30, 2024); IRS, Notice 2025-27, 2025-26 I.R.B. 1611 (June 23, 2025).

455 Exec. Order No. 14219, Ensuring Lawful Governance and Implementing the President's "Department of Government Efficiency" Deregulatory Initiative, 90 Fed. Reg. 10583 (Feb. 19, 2025).

digital assets to report information to the IRS and customers on the customers' sales of digital assets.[456] In addition to the broker reporting rules, the regulations provide substantive guidance for taxpayers to determine their basis, gain, and loss from digital asset sales. Treasury and the IRS have also published sub-regulatory guidance providing transition relief with respect to the information reporting regulations.[457] The IRS has issued a form and instructions on which brokers must report the information to the IRS and taxpayers.

Most recently, Treasury and the IRS have provided transition relief to U.S. digital asset exchanges and others implementing the digital asset broker regulations[458] and have withdrawn regulations that would have required certain DeFi participants to provide broker reporting in line with the passage of H.J. Res. 25.[459]

The section below covers the Working Group's priority items for the publication of guidance, along with priority legislative recommendations. The following sections discuss substantive tax issues, taxpayer reporting issues, and third-party information reporting.[460]

Substantive Tax Issues

Priority Guidance

CAMT

CAMT imposes a minimum tax generally equal to the excess, if any, of 15% of "adjusted financial statement income" (AFSI) less regular tax paid.[461] The calculation of AFSI generally starts with a corporation's net income as reported on its financial statement, subject to certain adjustments. CAMT applies generally to corporations with average AFSI over a three-year period of more than $1 billion and provides statutory adjustments to AFSI for financial statement income and losses resulting from stock and partnership investments. Regulations proposed in 2024 provide for additional adjustments for transactions where there are mismatches in financial statement or taxable income that distort true economic income (e.g., a hedging transaction in which only one side of the transaction is marked to market).[462]

Stakeholders have requested that Treasury and the IRS issue guidance to the effect that AFSI does not include financial accounting unrealized gains and losses on cryptocurrency, or on investments generally.

Priority Guidance

Treasury and the IRS should publish guidance addressing the determination of AFSI with respect to financial accounting unrealized gains and losses on investment assets other than stock and partnership interests. Toward this end, the IRS issued Notice 2025-27[463] stating that Treasury and the IRS anticipate interim guidance under CAMT to address how unrealized gains and losses on certain investment assets reported for financial statement purposes are considered for purposes of determining AFSI.[464]

456 Gross Proceeds and Basis Reporting by Brokers and Determination of Amount Realized and Basis for Digital Asset Transactions, 89 Fed. Reg. 56480 (July 9, 2024). A second regulation that was adopted in December 2024 addresses certain decentralized finance participants but no longer has force or effect. *See supra* notes 441, 442.

457 IRS, Notice 2024-56, 2024-29 I.R.B. 64 (July 15, 2024); IRS, Notice 2024-57, 2024-29 I.R.B. 67 (July 15, 2024); IRS, Rev. Proc. 2024-28, 2024-31 I.R.B. 326 (July 29, 2024); IRS, Notice 2025-7, 2025-5 I.R.B. 524 (Jan. 27, 2025).

458 IRS, Notice 2025-33, 2025-27 I.R.B. 4 (June 30, 2025).

459 Gross Proceeds Reporting by Brokers That Regularly Provide Services Effectuating Digital Asset Sales, 90 Fed. Reg. 30825 (July 11, 2025) (effectuating a change to the Code of Federal Regulations to reflect that 89 Fed. Reg. 106928 (Dec. 30, 2024) no longer has force or effect); *see supra* notes 441, 442.

460 Descriptions of market practices and the use of terminology used by digital asset participants in the following sections of this chapter are not intended as characterizations of those transactions for federal income tax purposes.

461 Section 10101 of Pub. L. No. 117-169, 136 Stat. 1818, 1818-1828 (2022) imposes the CAMT for taxable years beginning after December 31, 2022.

462 Corporate Alternative Minimum Tax Applicable After 2022, 89 Fed. Reg. 75062 (Sept. 13, 2024).

463 2025-26 I.R.B. 1611 (June 23, 2025).

464 IRS, Notice 2025-27, *supra* note 454.

Staking – Grantor Trust Classification

U.S. investment funds holding digital assets that qualify as exchange-traded products (ETPs) (pursuant to securities laws) are often organized as trusts. Typically, such funds take the position that they are classified for U.S. federal income tax purposes as investment trusts treated as grantor trusts. An investment trust is a type of legal-form trust that satisfies strict restrictions on its permitted activities and is consequently eligible to provide simplified tax reporting to its investors. A legal-form trust is classified as an investment trust rather than a business entity only if it is not engaged in a profit-making business. In addition, there may not be a power to vary the investments of the trust, and the trust may have only one class of ownership interests with a very limited exception.[465] Investors in an investment trust that is a grantor trust are treated as if they were the direct owners of their pro rata interests in trust assets for federal income tax purposes. They receive tax reporting from the trust or their brokers on IRS Forms 1099 (e.g., an IRS Form 1099-B, *Proceeds from Broker and Barter Exchange Transactions*, reporting gross proceeds and basis if the trust sells an asset). A legal-form trust that is intended to be structured as an investment trust treated as a grantor trust, but fails to satisfy the requirements for investment trust status, typically is classified as a partnership for federal income tax purposes. In this case, investors would receive tax reporting on Schedule K-1 of IRS Form 1065, *U.S. Return of Partnership Income*.

Stakeholders have requested guidance addressing whether a trust holding digital assets that stakes those assets and receives staking rewards can qualify as an investment trust treated as a grantor trust.[466]

Priority Guidance

Treasury and the IRS should publish guidance addressing whether a trust that otherwise qualifies as an investment trust treated as a grantor trust fails to qualify as such if the trust stakes digital assets owned by the trust.

Wrapping

Wrapping is a technique used to convert a digital asset native to one blockchain ("original digital asset") into a digital asset native to a different blockchain ("wrapped digital asset"). Wrapping may also be used to convert a digital asset that cannot be used in certain smart contracts into a wrapped digital asset that can be used in those smart contracts. The wrapped digital asset is backed one-for-one by the original digital asset, which is immobilized by a custodian or through smart contracts. The original digital asset may not be used in any transactions while it is wrapped. The wrapped digital asset can be unwrapped or be converted back to the original digital asset, at any time.

Wrapping is commonly used to transact with the value of the original digital asset on a different blockchain. An example is wrapped bitcoin, which can be used in DeFi operations, while bitcoin itself generally cannot. Stakeholders have asked for guidance addressing whether wrapping and unwrapping transactions are taxable transactions.

Priority Guidance

Treasury and the IRS should publish guidance addressing whether wrapping and unwrapping transactions are taxable transactions.

IRS FAQs

As described in the Current Tax Guidance on Digital Assets section above, the IRS issued FAQs on several issues involving digital assets starting in 2014. New FAQs have been added from time to time, but the FAQs have not been comprehensively revised to consider published guidance and regulations relating to digital assets.

465 *See* Treas. Reg. § 301.7701-4 (tax classification of trusts).

466 Stakeholders also have requested guidance on other issues relating to staking. See Chapter VII, Substantive Tax Issues: Priority Guidance – Other Issues. For a description of staking, see *Chapter II, Mining and Staking*.

Priority Guidance

Treasury and the IRS should update the IRS FAQs on digital assets. These updates will provide industry and taxpayers with regulatory certainty by reflecting guidance that was published after the issuance of the FAQs.

Other Issues

Stakeholders have requested guidance on several issues beyond those described above. The Working Group believes many of these issues might warrant future guidance in line with the goals of the Executive Order.

- **Mining and Staking.** Stakeholders have asked:
  - for clarification, modification, or reversal of IRS guidance on the timing of income from staking and mining rewards;[467]
  - whether staking activity constitutes a trade or business for federal income tax purposes and related questions including:
    - whether staking gives rise to income effectively connected with the conduct of a trade or business in the United States;
    - whether staking gives rise to unrelated business taxable income under Section 512;
    - whether staking gives rise to income from commercial activity for purposes of Section 892; and
    - whether income from staking is treated as fixed, determinable, annual or periodic income to foreign taxpayers;
  - the source of income from staking rewards;
  - whether the receipt of airdrops and hard forks invalidates investment trust status; and
  - whether staking benefits from the securities or commodities "trading safe harbors" of Section 864.
- **Valuation.** Guidance on how to value digital assets that are traded on multiple exchanges or thinly traded, for purposes of determining amount realized and basis.
- **NFTs.** Guidance on non-fungible tokens, including whether they are treated as collectibles for purposes of Sections 408(m) and 1(h)(5).
- **Losses on digital assets.** Guidance relating to losses on digital assets, including the standards and acceptable proof for worthlessness and abandonment and when losses may be deducted if they are held by a taxpayer that becomes bankrupt. Guidance relating to thefts of digital assets.
- **Charitable deductions.** Legislation removing the requirement for a qualified appraisal for charitable donations of digital assets worth more than $5,000.

In addition, many substantive issues that could be addressed either through future guidance or legislation include:

- Whether tokenization of an asset gives rise to a new asset for federal income tax purposes, and if so under what circumstances.
- The application of the investment company rules of Sections 351 and 721 to digital assets.
- Distributions of digital assets in partnership liquidations (the "marketable securities" rules).
- The application of the hot asset rules to sales of partnerships holding digital assets.

467 For further discussion of these issues, *see* Chapter VII, Taxpayer Reporting: Priority Guidance – *De Minimis Digital Asset Receipts* and Chapter VII, Taxpayer Reporting: Legislative Proposals for Other Issues – *Timing of Income from Mining and Staking*.

- Expanding the classes of assets that may be held by regulated investment companies to include digital assets.
- The treatment of digital assets for purposes of the subpart F, GILTI, and PFIC rules.
- The tax treatment of blockchain splits and blockchain mergers.
- The rules applicable to digital assets with respect to retirement accounts.
- The tax consequences of repatriation by an offshore foundation

Regarding offshore foundations, the Working Group encourages non-profit organizations supporting the development of blockchain technologies to domicile in the United States. Toward this end, the Working Group will engage with Treasury and the IRS to study ways to incentivize their repatriation and domestication.

Priority Legislative Recommendations

Characterization as Securities or Commodities

As described in the Current Tax Guidance on Digital Assets Section above, IRS Notices characterize virtual currency for federal income tax purposes as *property*, not currency. However, IRS guidance does not address whether a digital asset is considered a security or commodity for federal income tax purposes. The Code and case law define the term "security" in different ways for different tax purposes, and those definitions are not the same as the securities law meaning of the term "security." Code provisions also do not define the term "commodity" or define it in a circular manner, and do not cross-reference the commodities law meaning of the term. The characterization of an asset as a security or commodity for federal income tax purposes affects the application of multiple provisions of the Code. For example, Code provisions applicable to commodities include Section 475(e) and (f) (elections for dealers or traders in commodities to mark commodities to market), Section 864(b)(2)(B) (trading in commodities safe harbor), and Section 7704(d)(1)(G) (passive income exception applicable to commodities partnership).

Congress is considering legislation that would dictate when a digital asset is subject to regulation by the SEC or the CFTC, such as the Digital Asset Market Clarity Act of 2025 (CLARITY).[468] This legislation does not address the tax classification of digital assets. Adding digital assets, or in some cases actively traded fungible assets (the type of digital assets most similar to securities and commodities), as a new category of asset subject to Code provisions would permit legislation to consider characteristics of digital assets that are different from those of traditional securities or commodities. An alternative approach could be for a digital asset, or one or more types of digital assets, to be defined as a security or a commodity by reference to securities and commodities laws. Because the tax rules for securities and commodities differ in significant respects, it would be important that an asset have a single tax classification throughout its existence.

Recommendation

Legislation should be enacted that 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. Code provisions that should be expanded to apply to actively traded fungible digital assets include Sections 475 (mark-to-market election), 864(b) (trading safe harbors), 1058 (securities loans), and 7704 (publicly traded partnership rules).[469] In addition, Sections 1091 (wash sale rules) and 1259 (constructive sales) also should apply to digital assets. Alternatively, legislation could instead clarify when a digital asset commodity or other digital asset is treated as a security or a commodity for federal income tax purposes.

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

469 A 2023 report by the Joint Committee on Taxation discusses the current state of the law and possible legislation with respect to most of these provisions. Joint Committee on Taxation (JCT), *Selected Issues Regarding the Taxation of Digital Assets* (June 2023), https://www.finance.senate.gov/imo/media/doc/jct_report_on_digital_assets.pdf.

Stablecoins

As described in Chapter V, a stablecoin is a digital asset that intends to maintain a stable value relative to a reference asset, usually a currency. Most stablecoins are pegged to the U.S. dollar.[470] Stablecoins are widely used in digital asset transactions in a manner similar to a cash-equivalent, like shares in a money market fund. For example, a taxpayer may sell bitcoin for a stablecoin and later use the stablecoin to buy another digital asset. The Guiding and Establishing National Innovation for U.S. Stablecoins Act (GENIUS), which was signed into law on July 18, 2025, regulates the issuance of payment stablecoins in the United States.[471]

The tax characterization of stablecoins themselves under current law is uncertain. Characterization as debt, for example, is not certain—stablecoins typically do not have an unqualified obligation to pay a fixed amount, but they are held out as redeemable for cash. Under GENIUS, U.S.-licensed issuers of payment stablecoins are obligated to convert, redeem, or repurchase such stablecoins for a fixed amount of monetary value.[472] The payment stablecoins must also be collateralized with high quality liquid assets.[473]

The determination of a financial instrument's status as debt for federal income tax purposes is made under factors established by case law. A common requirement is for the instrument to have an unconditional promise to pay on demand, or on a specified date, a sum certain in money.[474] The instrument must also be evaluated based on other criteria established by case law, typically including whether the instrument pays interest, whether the issuer is adequately capitalized, whether the instrument is issued to a related party, and the seniority of the payment obligation. Payment stablecoins would satisfy the unconditional promise requirement and several of the other typical characteristics of debt. They also would have the economic characteristics of highly rated collateralized debt.

The expected use of payment stablecoins as financial assets that function in a manner similar to cash-equivalents raises the question of whether they could be considered as either money or currency for federal income tax purposes. Those terms are not defined by statute or case law, but Section 985(b)(1)(B) defines functional currency for certain purposes as the currency of the economic environment in which a significant part of a business unit's activities is conducted and which is used by such unit in keeping its books and records. The functional currency of a U.S. individual is always the dollar. Relatedly, a recent IRS Notice described "real" currency as (i) the coin and paper money of the United States or of any other country that is (ii) designated as legal tender, (iii) circulates, and (iv) customarily used and accepted as a medium of exchange in the country of issuance.[475] At present, stablecoins do not appear to satisfy these requirements. Stablecoins also are not issued by or guaranteed by any government.

Treatment of payment stablecoins as money or currency for federal income tax purposes does not seem likely under current law. Moreover, even if payment stablecoins were treated as currency, they could be nonfunctional currency for federal income tax purposes, in which case gain or loss on stablecoins would continue to need to be reported on tax returns. Treating payment stablecoins as money (and functional currency) would affect the application of many provisions of the Code in ways that may not be desirable. For example, the Code does not contemplate the possibility of gain or loss on money,[476] so no rules exist to deal with the possibility of gains or losses on payment stablecoins treated as money. In addition, treatment

470 *Supra* note 333.

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

472 S. 1582, 119th Cong. (2025) § 2(22)(A)(ii)(I) (enacted).

473 *See* S. 1582, 119th Cong. (2025) § 4(a)(i)(A) (enacted).

474 *See* 26 U.S.C. § 385(b)(1).

475 IRS, Notice 2014-21, *supra* note 445.

476 The Code has rules for gains or losses on functional currency transactions that are part of the ordinary business operations of a qualified business unit such as a branch, but those rules generally would not apply to the use of stablecoins by U.S. persons in the United States.

of payment stablecoins as money, as opposed to property, may affect basis and recognition of gain or loss to corporations, partnerships, and their owners in the context of distributions and contributions of payment stablecoins.[477]

If payment stablecoins were treated as debt for federal income tax purposes, they would be subject to multiple provisions of the Code that apply to debt. They may also be subject to provisions applicable to securities as defined for federal income tax purposes (which is independent of the securities law definition of that term), depending on which tax definition of security is applicable. Treatment of a payment stablecoin as a security is a separate and additional inquiry from characterization as debt.

Among the Code provisions that could apply to payment stablecoins treated as debt are (i) the wash sale loss disallowance rules of Section 1091, and (ii) the anti-bearer bond rules applicable to registration-required obligations that are not in registered form.[478] As discussed in Chapter V, while stablecoins today are primarily used to facilitate trading in other digital assets, they could be more widely adopted as forms of payment in the future. Stablecoins can diverge from their pegs and can therefore give rise to loss on disposition when used to make payments. This would implicate the wash sale rules.

To the extent that stablecoins are used as forms of payment, applying the wash sale rules would be difficult to administer and yield very little tax unless the taxpayer were transacting in large amounts. There may also be limited utility in applying the wash sale rules to dispositions of small amounts of stablecoins in trading activities.[479] Application of the anti-bearer bond rules would make stablecoins impractical for several reasons, including that U.S. issuers would be subject to an excise tax. That said, stablecoins function somewhat like bearer bonds since they are readily tradable and held in a way that does not identify the owner.

Recommendation

Legislation should be enacted that would characterize payment stablecoins for federal income tax purposes, as such matters are not addressed by GENIUS. Characterization as debt seems most appropriate given the ways in which payment stablecoins are structured and the potential for gain or loss on disposition. If payment stablecoins are treated as debt, the legislation should also consider the applicability of existing federal income tax rules that could impede the widespread use of payment stablecoins as financial assets that function in a similar manner to cash-equivalents. In particular, legislation should address the wash sale and anti-bearer bond rules. To address the wash sale rules, possible options include:

- Providing that the wash sale rules do not apply to payment stablecoins;
- Providing that the wash sale rules do not apply to de minimis losses from payment stablecoins, possibly up to an aggregate threshold;[480] or
- Providing that gains and losses on payment stablecoins are not considered for federal income tax purposes.

477 As discussed in Third-Party Information Reporting: Other Issues – *Digital Assets Received in a Trade or Business*, below, the treatment of digital assets as cash for purposes of Section 6050I has raised a number of concerns by taxpayers.

478 The anti-bearer bond rules are in Sections 149(a), 163(f), 165(j), 312(m), 871(h), 881(c), 1287, and 4701.

479 The digital asset reporting rules that apply to U.S. digital asset exchanges and other brokers do not require brokers to report dispositions of stablecoins to buy other digital assets, and do not require reporting of dispositions of stablecoins for cash unless aggregate dispositions of stablecoins during a calendar year exceed $10,000. These rules apply only for broker reporting purposes, not for purposes of taxpayer determinations of gain or loss on stablecoin transactions.

480 Stakeholders have urged that either Congress or the IRS adopt a broader de minimis rule. *See infra* note 488 for a discussion of possible legislation on this topic.

If no such legislation is enacted, Treasury and the IRS should consider issuing guidance that would clarify the tax classification of payment stablecoins, and address the potential application of the wash sale[481] and anti-bearer bond rules.[482]

Wash Sales

Because wash sale rules apply to securities, they would not apply to digital assets that are not securities. Taxpayers with loss positions in digital assets are engaging in transactions that would be subject to the wash sale rules if the digital assets were subject to Section 1091. For example, a taxpayer may sell a digital asset at a loss on one day and repurchase the same digital asset the next day, claiming the loss for tax purposes while being in a substantially similar position economically.

Recommendation

The wash sale rules should be amended to add digital assets to the list of assets subject to the wash sale rules.[483] If legislation of this kind is enacted, the broker reporting regulations should be amended to reflect these changes to the wash sale rules. As previously discussed, the wash sale rules should not apply to payment stablecoins.

Crypto Lending

Pursuant to Section 1058, loans of securities ordinarily are treated as an exchange of the security for an obligation to return the security on which no gain or loss is recognized. This is contingent upon the transfer of the security being pursuant to an agreement that meets certain requirements. Gain or loss is not recognized on the return of that security in exchange for rights under the agreement. The agreement must (i) provide for the return to the transferor of securities identical to the securities transferred; (ii) require that payments be made to the transferor of amounts equal to all interest, dividends and distributions on the security during the term of the securities loan; (iii) not reduce the risk of loss or opportunity for gain of the transferor in the transferred securities; and (iv) meet such other requirements as the Secretary of the Treasury may prescribe. These rules are intended to ensure that the taxpayer making the loan of securities remains in an economic and tax position similar to the position it would have been in absent the loan.

In a transaction commonly referred to as a crypto loan, a taxpayer (the original digital asset owner) transfers a digital asset to a third party transferee either directly or indirectly (such as through a centralized platform, or through the use of an automatically executing smart contract), subject to an obligation (or the provisions of the automatically executing smart contract) for the transferee to deliver the same type of digital asset back to the original digital asset owner in the future. At a later date, the transferee delivers the same type of digital asset to the original digital asset owner. The transferee may also deliver or credit additional digital assets or other consideration to the original digital asset owner as compensation for the use of the digital asset during the transaction.[484]

481 IRS, Rev. Proc. 2014-45, 2014-34 I.R.B. 388 (Aug. 18, 2014) and IRS, Rev. Proc. 2023-35, 2023-42 I.R.B. 1079 (Oct. 16, 2023) provide that the IRS will not treat a redemption of shares in a money market fund as part of a wash sale. Revenue Procedure 2014-45 states that a money market fund is often used as an account into which, or from which, cash is automatically deposited or withdrawn, under a sweep arrangement. The Revenue Procedures relieve tax administration burdens attributable to changes in SEC rules that made it more likely that money market fund shares would be redeemed at a loss. If no legislation addressing the tax treatment of payment stablecoins is enacted, Treasury and the IRS could consider issuing similar guidance with respect to payment stablecoins under a similar tax administration rationale.

482 If legislation is not enacted, Treasury and the IRS could consider whether it is possible to issue guidance concluding that payment stablecoins are not registration-required. Obligations are registration-required unless one of three exceptions applies. Section 163(f)(2).

483 Proposed wash sale legislation expanding the scope of the wash sale rules to cover digital assets has previously been considered, and was scored as raising $26 billion over 10 years, although that version of the legislation also included non-digital asset provisions. Office of Management and Budget, Budget of the U.S. Government: Fiscal Year 2025 163 (Mar. 11 2024), https://www.whitehouse.gov/wp-content/uploads/2024/03/budget_fy2025.pdf.

484 *See* Chapter II, Market Activities: Lending, Borrowing, and Collateral (discussing cryptocurrency lending).

Taxpayers may engage in crypto borrowing and lending transactions for reasons similar to those for securities lending, or in transactions that may be conceptually similar to borrowing cash on a collateralized basis. That said, crypto lending transactions may differ in a number of regards from securities loans. For example, the loan may be effected purely through smart contracts, with automatically executing software replacing a traditional legal agreement. Further, amounts received (typically, airdrops) on the loaned asset are not necessarily passed back to the lender.

Section 1058 does not apply to loans of digital assets, unless the asset constitutes a security for federal income tax purposes. Stakeholders have requested guidance to the effect that crypto loans are treated as transactions in which no gain or loss is recognized under circumstances similar to those provided by Section 1058.

Loans of digital assets that satisfy requirements similar to the Section 1058 conditions described above should be accorded similar treatment. While the Working Group understands that some market participants take the position that loans of digital assets that meet similar conditions are non-taxable, no authority directly addresses those transactions. As such, there is uncertainty for taxpayers on this crucial question.[485] Moreover, crypto lending transactions may not be carried out in a way that fully complies with the requirements of Section 1058, as described above, and the enactment of Section 1058 may have limited the extent to which prior non-statutory law applies to loans of securities or other assets.

Recommendation

Legislation should be enacted to amend Section 1058 to provide that it applies to loans of actively traded fungible digital assets, provided that the loan has terms similar to those currently required for loans of securities. The Secretary of the Treasury should be granted authority to determine when a digital asset is actively traded, and to address differences between the standard terms of securities loans and crypto loans.

Mark-to-Market Rules

Traders in securities, and dealers and traders in commodities, may elect to mark their securities or commodities to market for federal income tax purposes. No guidance addresses the extent to which these rules apply to digital assets.

Recommendation

See the *Characterization as Securities or Commodities* discussion above, which recommends amending Section 475 to include actively traded fungible digital assets.

Trading in Securities or Commodities Safe Harbors

Non-U.S. traders in securities or commodities may trade through an independent U.S. agent, or trade for their own account with U.S.-based personnel, without being treated as engaged in the conduct of a trade or business in the United States. This precludes them from the obligation to file U.S. income tax returns due to those trading activities, provided that certain conditions are met. These safe harbors do not apply to digital assets unless they qualify for federal income tax purposes as securities or commodities and those conditions are met. While the Working Group acknowledges that some market participants take the position that certain digital assets are treated as commodities for federal income tax purposes, no authority directly addresses whether trading in those assets satisfies the commodities trading safe harbor.[486]

Recommendation

See the *Characterization as Securities or Commodities* discussion above, which recommends amending Section 864(b)(2) to include actively traded fungible digital assets.

485 *See generally* JCT, *supra* note 469.

486 *Id.*

Taxpayer Reporting

Priority Guidance

De Minimis Digital Asset Receipts

It is common for taxpayers holding digital assets to receive or have the opportunity to receive new digital assets that may have minimal or speculative value. For example, taxpayers who delegate their rights to stake to others who validate transactions may receive frequent small rewards. A taxpayer may also receive unsolicited airdrops of, or claims to, a newly created digital asset as a marketing promotion by the creators of the new digital asset. These assets may be illiquid and therefore hard to value. In practice, it appears that they frequently lose value shortly after the drop. When a hard fork of a digital asset takes place, the new digital asset's value is often uncertain for a period of time and may rapidly decline.

Under applicable law and current IRS guidance,[487] taxpayers must include the fair market value of these assets in income when they have dominion and control over the asset. Digital asset exchanges have different practices as to when they make a new asset available to customers. As such, a customer of multiple exchanges may acquire dominion and control over a new asset at different times as a result of the exchanges' varied practices.

These fact patterns give rise to administrative burdens to taxpayers to track and record each event. At times, these burdens may exceed the value of the transactions. These burdens arise from one or more of: (i) high volume but low value assets, (ii) valuations that change rapidly, typically with a loss of value, and (iii) questions about the precise moment a taxpayer has dominion and control over a new asset given differences in how digital asset exchanges operate. Moreover, in the fact patterns described above, taxpayers often have a limited ability to influence when a new asset or the right to obtain a new asset appears.

Priority Guidance

Treasury and the IRS should issue administrative guidance that addresses de minimis receipts of digital assets.[488] The guidance could apply to airdrops, staking, hard forks, and mining rewards for taxpayers who do not operate a node or carry out digital asset mining.

Legislative Proposals for Other Issues

Timing of Income from Mining and Staking

The receipt of cash or property for services generally is taxable as ordinary income at the time of receipt. For property received for services, the taxpayer generally includes the fair market value of the property on the date received in gross income. The basis of property in the hands of the taxpayer is the amount included in gross income.

487 When a taxpayer successfully "mines" virtual currency, the fair market value of the virtual currency as of the date of receipt is includible in gross income. IRS, Notice 2014-21, *supra* note 445. The IRS has stated that if a cash method taxpayer stakes cryptocurrency native to a proof-of-stake blockchain and receives additional units of cryptocurrency as rewards when validation occurs, the fair market value of the validation rewards is included in the taxpayer's gross income in the taxable year in which the taxpayer gains dominion and control over the validation rewards. IRS, Revenue Ruling 2023-14, *supra* note 448.

488 Stakeholders have urged that taxpayers should not be required to include in income de minimis gains from digital assets, or digital assets used for personal transactions, by analogy to the rules for personal foreign currency transactions by individuals under Section 988(e). Some bills previously introduced in Congress have provided for a de minimis inclusion rule. Because digital assets are used for investment or speculation as well as payment, the rationale for the current exclusion under Section 988(e) is not equally applicable to digital assets. There are better arguments to exclude de minimis gains or losses for digital assets used primarily for payments (see the stablecoins discussion above). However, any de minimis rule for including gains and losses from digital assets in income would pose complications that are not relevant in the most common fact patterns where individuals dispose of foreign currency. Unless an individual lives outside the United States, the likely fact pattern for disposing of foreign currency is when a taxpayer is on vacation for a limited period of time, in which case it is easy to determine that the transaction is a personal one and it is likely often to be the case that gain from the disposition is under the statutory threshold as a practical matter. By contrast, digital assets are also used in investment or trading transactions and the same type of digital asset may be used by the same taxpayer for both investment and payment purposes. If a legislative de minimis rule were modeled on Section 988(e), questions would include: how taxpayers would distinguish personal from investment/ trading transactions and what records would be considered adequate in that regard; whether an aggregation rule should apply so that taxpayers cannot split a large transaction into multiple small ones; whether there would be any constraints on taxpayers' ability to treat gain transactions as non-taxable personal transactions but loss transactions as investment or business transactions; and how brokers should report transactions if they do not know whether the transaction is personal or not. This list is not exclusive and would change if a legislative de minimis rule were drafted in a way that differs from Section 988(e).

In contrast, income with respect to certain self-created property such as manufactured goods, farmed crops, and certain self-created intellectual property generally is not realized until the property is sold or otherwise disposed of. Treasury and the IRS have issued guidance stating that when a taxpayer successfully "mines" virtual currency, the fair market value of the virtual currency as of the date of receipt is includible in gross income.[489] In addition, Treasury and the IRS have issued guidance holding that if a cash method taxpayer stakes cryptocurrency native to a proof-of-stake blockchain and receives additional units of cryptocurrency as rewards when validation occurs, the fair market value of the validation rewards is included in the taxpayer's gross income in the taxable year in which the taxpayer gains dominion and control over the validation rewards.[490] Stakeholders have asked for clarification, modification, or reversal of this IRS guidance on the timing of income from mining and staking rewards.

Possible Guidance

In light of these stakeholder requests and given the significant growth and maturation of digital assets and surrounding infrastructure since the issuance of guidance in 2014, 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, taking into account any recent intervening developments since the issuance of such guidance.

Possible Legislation

Several bills have been introduced in Congress to change the timing of income from mining and staking rewards and several other bills have been proposed. For example, H.R. 8149 (2024) proposed to defer the inclusion of validation rewards until the year of the sale or other disposition of the rewards. By contrast, other bills, such as the Responsible Financial Innovation Act, S. 2281 (2023) proposed only to defer the inclusion of de minimis amounts of income relating to mining or staking until the year of the sale or other disposition of the digital assets.

If Congress decides to pass legislation regarding the timing of the inclusion of income relating to mining or staking, Congress should consider whether similar rules should apply to rewards from other digital asset validation methods, what the character of income upon disposition should be and if ordinary, what rules should apply to determine the order of dispositions of ordinary versus capital units, and potential differences between the fair market value of rewards at the time of receipt compared with the fair market value of rewards at the time of sale or other disposition.

Section 6038D Digital Asset Reporting

Section 6038D requires an individual that holds an interest in one or more specified foreign financial assets with an aggregate value of at least $50,000 during a taxable year to attach a statement with required information to the individual's tax return. A specified foreign financial asset means a financial account maintained by a foreign financial institution and certain specified foreign assets not held in a financial account maintained by such a financial institution. Penalties apply to taxpayers who fail to provide the required information, and the time for IRS assessment of tax and the statute of limitations for assessment are extended beyond the deadlines that otherwise apply. These rules allow the IRS to cross-check the information that it receives from U.S. taxpayers against the information that it receives from foreign financial institutions about U.S. customer accounts pursuant to the Foreign Account Tax Compliance Act (FATCA) of the Hiring Incentives to Restore Employment Act of 2010, Pub. L. No. 111-147, 124 Stat. 71 (2010). Section 6038D does not explicitly refer to digital asset accounts.

489 IRS, Notice 2014-21, *supra* note 445; *see also Statement on Certain Proof-of-Work Mining Activities*, SEC Division of Corporation Finance (Mar. 20, 2025), https://www.sec.gov/newsroom/speeches-statements/statement-certain-proof-work-mining-activities-032025.

490 IRS, Revenue Ruling 2023-14 (July 31, 2023), https://www.irs.gov/pub/irs-drop/rr-23-14.pdf; *see also Statement on Certain Protocol Staking Activities*, SEC Division of Corporation Finance (May 29, 2025), https://www.sec.gov/newsroom/speeches-statements/statement-certain-protocol-staking-activities-052925.

U.S. taxpayers can transact with offshore digital asset exchanges and wallet providers without leaving the United States. The global nature of the digital asset market offers opportunities for U.S. taxpayers to conceal assets and taxable income by using offshore digital asset exchanges and wallet providers. As a result, taxpayers who wish to hide their assets from the IRS in an offshore account may have an incentive to hold digital assets rather than traditional financial assets, which could distort financial markets and undermine the effectiveness of the reporting required by Section 6038D.

As described in the section below titled "Crypto-Asset Reporting Framework Implementation," pursuant to a recently adopted international tax reporting standard, many foreign countries are in the process of adopting rules that will require that crypto-asset service providers report certain transactions by foreign customers to the tax administration or agency of the service provider's jurisdiction, which would then exchange appropriate information with other similar jurisdictions. This could include the United States.

Possible Legislation

Legislation could be enacted that would require taxpayers to report foreign digital asset accounts. A foreign digital asset account would be a custodial account that holds digital assets that is maintained by a foreign digital asset exchange or other foreign digital asset service provider. If the United States implements the Crypto-Asset Reporting Framework (CARF), taxpayers could be required to report accounts with foreign crypto-asset service providers that are required to report information on U.S. customers to a non-U.S. tax authority. This would allow the IRS to cross-check the information that it receives from U.S. taxpayers with the information it would receive from foreign digital asset exchanges about U.S. customer accounts. Providing the Secretary with authority to coordinate this provision with other rules could mitigate duplication or minimize burden with respect to other types of reporting rules.

Section 6038D and FBAR Reporting

The information required to be reported under Section 6038D on IRS Form 8938, Statement of Specified Foreign Financial Assets, is similar to information that many taxpayers are required to report under 31 U.S.C. § 5314 and the regulations published thereunder on a form known as a Report of Foreign Bank and Financial Accounts, or an FBAR, resulting in some duplicative reporting. The Form 8938 is filed with the IRS. The FBAR is filed with the Treasury Financial Crimes Enforcement Network (FinCEN). If reporting under Section 6038D and on the FBAR are expanded to require reporting of digital asset holdings, more taxpayers would be subject to these duplicative reporting obligations.

Possible Legislation

Legislation could be enacted that would streamline the reporting required under Section 6038D and on the FBAR. Legislation could permit a taxpayer that is subject to both reporting obligations to submit a single form that would be available both to the IRS and to FinCEN. This could be accomplished by amending 31 U.S.C. § 5314 and 26 U.S.C. § 6038D so that the reporting requirements under both titles match, similar to how 31 U.S.C. § 5331 and 26 U.S.C. § 6050I both require reporting on certain large cash payments on FinCEN/IRS Form 8300. If the form is submitted as an attachment to a federal income tax return, for tax administration reasons this option should be available only to taxpayers that use a calendar taxable year and file tax returns electronically. Consideration could be given to conforming the information required to be reported and the different reporting thresholds and penalties that currently apply with respect to Section 6038D reporting and FBARs, and, if necessary, to further amending the Code to allow the IRS to provide the reported information to FinCEN. To the extent that single-filing legislation is enacted, resources should be provided to the IRS sufficient to carry out the reprogramming of its systems necessary to implement the legislation.

Third-Party Information Reporting

Priority Guidance

Electronic Furnishing of Digital Asset Payee Statements (Form 1099-DA)

Third parties that report information to the IRS are also generally required to provide or furnish a copy of that information to the relevant taxpayer. These documents are referred to as payee statements. The default rule for furnishing payee statements to taxpayers is in paper format. Payee statements can be furnished to taxpayers in electronic format only with taxpayer consent, which must be provided by the taxpayer in the manner required by the IRS. Current rules provide that the taxpayer must have affirmatively consented to receive the copy in electronic format.[491] The consent requirement is intended to ensure that taxpayers have the capacity and willingness to receive payee statement electronically.

Unlike traditional financial institutions, digital asset exchanges communicate with their customers exclusively electronically. Customers have therefore demonstrated that they are able to obtain the information they need from digital asset exchanges electronically. Requiring digital asset exchanges to send customers a copy of IRS Form 1099-DA, *Digital Asset Proceeds From Broker Transactions*, in paper form unless a customer affirmatively consents to electronic delivery imposes unnecessary and burdensome costs on brokers serving the digital asset space.

Priority Guidance

Treasury and the IRS should propose regulations that provide brokers that facilitate sales or exchanges of digital assets through electronic means with a less burdensome method of obtaining consent from their customers to furnish Form 1099-DA payee statements in an electronic format.

Crypto-Asset Reporting Framework Implementation

When a U.S. taxpayer sells securities, its U.S. broker provides reporting about the sale on IRS Form 1099-B. The reporting goes to the IRS with a copy to the selling taxpayer. Historically, taxpayers wishing to avoid IRS scrutiny did so by holding their cash and securities investments with offshore banks that actively solicited U.S. customers and had no obligations to report information to the IRS. To address this problem, the IRS has received information since 2015 from certain foreign jurisdictions on financial accounts that U.S. taxpayers maintain at foreign financial institutions. In exchange, the IRS provides information to many of those foreign jurisdictions on financial accounts held by residents of those jurisdictions at U.S. financial institutions, provided the recipient jurisdiction satisfies certain data confidentiality and security conditions.

As with securities, jurisdictional arbitrage presents a key tax evasion risk for digital assets. The ease of cross-border transfer and access to offshore exchanges enables U.S. taxpayers seeking to evade their tax obligations an offramp to do so. As the ecosystem matures in the United States, leaving these pathways untouched would create a structural disadvantage for brokers and exchanges domiciled in the United States.

Other countries have similar concerns about the potential for their taxpayers to carry out digital asset transactions in a way that avoids domestic tax scrutiny by moving their assets offshore. The Crypto-Asset Reporting Framework (CARF) is an international tax transparency standard that seeks to improve tax

491 Section 401 of the Job Creation and Worker Assistance Act of 2002, Pub. L. No. 107-147, 116 Stat. 21 (2002) provides that any person required to furnish a payee statement under certain information reporting provisions of the Code (including Section 6045) may electronically furnish such statement to any recipient who has consented to the electronic provision of the statement in a manner similar to the one permitted under regulations issued under Section 6051 of the Code or in such other manner as provided by the Secretary. The rules that currently apply to furnishing payee statements electronically under Section 6045 are based on the Section 6051 regulations, which apply to furnishing employee statements on Forms W-2. *See* IRS, Pub. No. 1179, General Rules and Specifications for Substitute Forms 1096, 1098, 1099, 5498, and Certain Other Information Returns (July 22, 2024), https://www.irs.gov/pub/irs-pdf/p1179.pdf.

compliance for transactions involving digital assets by requiring that digital asset service providers report certain transactions to the tax administration or agency of the provider's jurisdiction, which would then exchange appropriate information with other jurisdictions participating in CARF. As of May 2025, more than 65 jurisdictions have committed to implementing CARF. U.S. implementation of CARF pursuant to Section 6045 would allow the IRS to obtain information on digital asset transactions of U.S. taxpayers in foreign jurisdictions by collecting and exchanging information on U.S. transactions of residents of those jurisdictions.

U.S. regulations implementing CARF would discourage U.S. taxpayers from moving their digital assets to offshore digital asset exchanges. Implementing CARF would promote the growth and use of digital assets in the United States and alleviate concerns that the lack of a reporting program could disadvantage the United States or U.S. digital asset exchanges.

However, U.S. digital asset exchanges are currently implementing regulations under Section 6045 that will require those exchanges to start reporting information on 2025 sales and exchanges of digital assets by U.S. customers in 2026, with additional stages of reporting and backup withholding coming into effect after 2025. In order to minimize burdens on U.S. digital asset exchanges, any new reporting obligations on U.S. digital asset exchanges should take into account both the timing of the rollout of reporting and withholding obligations under the existing regulations and also coordination with the operative rules of the existing regulations, for example the identification of entities subject to reporting, the types of assets and transactions required to be reported, and the procedures for customer due diligence that must be carried out.

Priority Guidance

Treasury and the IRS should consider proposing regulations to implement CARF that take stakeholder concerns into account and minimize burdens on brokers to the extent consistent with CARF rules. The proposed regulations should not impose any new reporting requirements on DeFi transactions and should be used as a forum to gather further feedback, including a reasonable timetable for implementation.

Other Issues

Basis Reporting on Transferred Digital Assets

Digital asset exchanges that are brokers for federal tax information reporting purposes are required to report information to the IRS and to taxpayers on the gross proceeds from sales of digital assets, for transactions on or after January 1, 2025, and the basis of certain digital assets sold, for transactions on or after January 1, 2026.[492] The combination of gross proceeds and basis information is necessary for taxpayers and the IRS to determine the taxpayers' gain or loss from the digital asset sale. Without basis information, broker reporting to customers would provide an incomplete picture, because it would identify transactions carried out by customers and gross proceeds received but not gain or loss. Reporting of that kind is likely to be confusing to customers, who would not receive the full information they need to properly report transactions on their income tax returns. Because the IRS would not receive basis information, this could result in IRS audits of tax-compliant taxpayers who correctly took basis into account on their tax returns. Accurate basis reporting is thus essential to preventing and identifying tax evasion and tax avoidance and prioritizing enforcement resources.

Under the final regulations, digital asset exchanges are required to report basis only if they have reliable basis information—namely where the taxpayer acquired, held and sold the digital asset at that exchange. However, taxpayers frequently transfer digital assets in and out of accounts at exchanges, so it is common for a taxpayer to acquire an asset with one exchange but then sell or exchange it through a second exchange. In recognition

492 At the request of industry, brokers are provided with an additional year to develop basis tracking systems, which are more difficult to build than the gross proceeds reporting systems.

of this common practice, the 2021 Infrastructure Investment and Jobs Act (IIJA) amended Section 6045A to require reporting of basis information when digital assets are transferred to digital asset exchanges that are brokers. These requirements are already in place when securities are transferred to or from securities brokers. When a taxpayer buys a security at one broker and later transfers the security to a second broker, the first broker must provide basis and other information to the second broker, but not to the IRS, on a transfer statement. As a result, if the taxpayer later sells the security through the second broker, the second broker can report to the taxpayer and the IRS both the gross proceeds of the sale and the basis of the security sold.

Transfers between centralized digital asset exchanges are similar in kind to the transfers of securities described above. The IIJA amendment to Section 6045A provides for transfer statements when digital assets are transferred to a digital asset exchange that is a broker. Implementing this legislation would improve the quality of the tax information taxpayers will receive from digital asset exchanges when they sell digital assets, by providing reliable basis information to those exchanges with respect to digital assets transferred to one digital asset exchange from another digital asset exchange.

Possible Regulations

Treasury and the IRS should consider proposing regulations requiring basis information to be reported when digital assets are transferred between centralized digital asset exchanges.

Digital Assets Received in a Trade or Business

If a trade or business receives more than $10,000 of cash in a transaction for, among other things, goods or services, the business generally must report that information to the IRS and to FinCEN. These coordinating rules are intended to detect and prevent tax evasion and financial crimes. Existing rules permit taxpayers to use the same form to report information to either the IRS or FinCEN, instead of to both agencies, which reduces the burden on filers.

The IIJA expanded the scope of reporting to the IRS by requiring reporting if a taxpayer uses digital assets to make payment. The implicit premise of this expansion is that using digital assets to pay for real-world goods and services normally purchased with money has the same effect as converting the digital assets to cash (which is required to be reported to the IRS) and using the cash to pay for the goods and services (which is also required to be reported to the IRS). The IIJA did not expand FinCEN's corresponding rule requiring the filing of reports that are highly useful to law enforcement.[493] This discrepancy causes disparate treatment of the use of digital assets to pay for goods and services.

Stakeholders have raised privacy and other concerns about the IIJA amendment. One concern is that reporting by, for example, certain service providers may reveal personal information to the IRS that it otherwise would not have. Another concern expressed by stakeholders is that the amendment could apply not only to the use of digital assets for traditional goods and services, but also to crypto-native transactions such as the swapping of one digital asset for another. A third concern that stakeholders have raised is that the amendment could provide a disincentive for taxpayers to use digital assets in the ordinary course of commerce, considering the current statutory dollar threshold.

Possible Regulations

Treasury and the IRS should consider proposing regulations implementing reporting of digital assets paid to a trade or business in a manner that takes the stakeholder concerns described above into account.

493 Additional information on FinCEN's reporting rules under the BSA are included in Chapter VI.

Possible Legislation

Consideration should be given to legislation to conform the information required to be reported to FinCEN, for BSA purposes, and the IRS, for federal income tax purposes. The legislation could also reexamine the reporting dollar thresholds and the breadth of uses of digital assets to which this provision would apply. Additional proposals related to the Form 8300 are included in Chapter VI.

Legislative Proposal for Other Issue

Implementation of CARF

A well-known technique used to avoid tax reporting by a financial institution or broker is to invest through a shell company. CARF provides that digital asset exchanges should identify and report on the controlling person of certain passive entities. The IRS does not have authority to require digital asset exchanges to report on controlling persons of many shell companies and therefore cannot provide that information to other countries.

A number of major trading partners of the United States are unwilling to provide information on U.S. persons who control shell companies carrying out digital asset transactions on foreign exchanges if those trading partners do not receive similar information from the IRS. Enactment of legislation that would permit the IRS to require U.S. digital asset exchanges to report information on foreign controlling persons of shell companies would ensure that the IRS could obtain similar information on U.S. taxpayers that control shell companies.

Possible Legislation

Legislation could require digital asset brokers to report information on foreign controlling persons of certain passive entities.

Table of Recommendations

Digital Asset Market Structure		
Recommendation	Policy Responsibility	
	Congress	Regulator
Enabling the Trading of Digital Assets at the Federal Level		
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.		SEC
The SEC should consider using its rulemaking and exemptive authority under the Exchange Act to advance the following initiatives: ▪ Enable non-security digital assets 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. ▪ 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 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.		SEC

Digital Asset Market Structure		
Recommendation	Policy Responsibility	
	Congress	Regulator
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.		SEC
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 spot retail commodity transactions on digital assets pursuant to CEA section 2(c)(2)(D). ▪ Provide guidance as to how digital assets may be considered commodities under Section 1a(9) of the CEA. For example, the agency can consider expanding upon prior guidance on "actual delivery" of virtual assets. ▪ 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. 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, 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) 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.		CFTC

Digital Asset Market Structure		
Recommendation	Policy Responsibility	
	Congress	Regulator
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.		SEC, CFTC
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.		SEC, CFTC
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).		CFTC, SEC
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.		SEC, CFTC
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.		CFTC
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. ▪ 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.		SEC, CFTC

Digital Asset Market Structure		
Recommendation	Policy Responsibility	
	Congress	Regulator
Creating a Lasting Framework for Digital Asset Market Structure		
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. ▪ The SEC and CFTC should adopt rules ensuring customer asset segregation for digital assets. ▪ 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	SEC, CFTC
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.	Congress	
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.	Congress	SEC, CFTC
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.	Congress	SEC, CFTC

Digital Asset Market Structure		
Recommendation	Policy Responsibility	
	Congress	Regulator
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.	Congress	CFTC
▪ 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.	Congress	
▪ 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.).	Congress	
▪ 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.	Congress	
▪ 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.	Congress	
▪ 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.	Congress	
▪ Intermediaries offering digital asset services should pay fees equivalent to those that traditional finance intermediaries pay in the equity markets.		

Digital Asset Market Structure		
Recommendation	Policy Responsibility	
	Congress	Regulator
SEC and CFTC registrants should be required to adopt best practices for cybersecurity standards.	Congress	
▪ These standards may be adopted as part of a principles-based regulatory framework or proposed as industry best practices.		
Regulatory Treatment of DeFi		
As contemplated in provisions of CLARITY, Congress should consider the following factors when determining the regulatory treatment of DeFi:	Congress	
▪ 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. ◦ 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.		

Digital Asset Market Structure		
Recommendation	Policy Responsibility	
	Congress	Regulator
Accounting Recommendations		
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. ▪ 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.		FASB

Banking and Digital Assets		
Recommendation	Policy Responsibility	
	Congress	Regulator
Current Regulatory Framework		
Relaunch agency crypto innovation efforts—as appropriate—to address outstanding bank activities.		FRB, FDIC, OCC
▪ 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, 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, 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, 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. ◦ *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.		FRB
▪ 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.		

Banking and Digital Assets		
Recommendation	Policy Responsibility	
	Congress	Regulator
Develop guidance and best practices to support banks and supervisors that is technically sound and principles-based.		FRB, FDIC, OCC, Commerce
▪ 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. 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		
Clarify the role of supervisors and banks in offering banking services to potential customers.		FRB, FDIC, OCC
▪ 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. ▪ 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. ▪ 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.		
Access to Providing Banking Services		
Provide clarity and transparency regarding the process for eligible institutions to obtain a bank charter or a Reserve Bank master account.		FRB, FDIC, OCC
▪ The relevant Banking Agencies should clarify and define in regulation the expected timelines for decision-making on completed applications for charter licensing (including federal deposit insurance where applicable) and requesting a Reserve Bank master account. ▪ If regulatory timelines are not met for a given application, the application should be deemed approved absent extraordinary circumstances. ▪ The Banking Agencies should also confirm that otherwise eligible entities are not prohibited from obtaining bank charters, obtaining federal deposit insurance, or receiving Reserve Bank master accounts or services solely because they engage in digital asset-related activities. ▪ Finally, the Banking Agencies should provide additional transparency, as appropriate, on the number of, and average time to review, complete applications, including new charter applications, federal deposit insurance applications, and Reserve Bank master account applications, on both an aggregated and annual basis.		

Banking and Digital Assets		
Recommendation	Policy Responsibility	
	Congress	Regulator
Capital and Other Applicable Regulatory Treatment		
The Banking Agencies should clarify the circumstances, using risk-based guidelines, under which tokenized assets and tokenized asset collateral would be subject to the same capital and liquidity treatment as the underlying asset or collateral.		FRB, FDIC, OCC
The United States should adopt capital requirements for bank digital asset activities that accurately reflect the risk of the asset or activity. Additionally, the United States should advocate that the BCBS revisit the cryptoasset standards to ensure similar treatment to U.S. capital requirements.		FRB, FDIC, OCC
Simplification of the cryptoasset grouping. ▪ BCBS's four groups of cryptoassets should be simplified. Applying a separate classification to traditional assets due to the use a specific technology does not adhere to the principle of technology-neutrality. Furthermore, the treatment of tokenized traditional assets as cryptoassets is misleading and may create unintended negative consequences. Additionally, the BCBS distinction between Group 2a and Group 2b cryptoassets does not create a clear enough distinction between cryptoassets widely used for payment and investment purposes and other cryptoassets, such as memecoins. ▪ The U.S. prudential cryptoasset framework should: (i) clarify when tokenized traditional assets are equivalent to traditional assets and are subject to the same capital and liquidity requirements as traditional assets; (ii) work to align the BCBS definition of stablecoins eligible for Group 1b treatment with requirements set forth in GENIUS; and (iii) simplify the classification of Group 2 cryptoassets and address the treatment of cryptoassets outside of Group 2.		FRB, FDIC, OCC
Use of permissionless blockchain for all groups of cryptoassets. ▪ Under the BCBS standards, cryptoassets relying on permissionless blockchains pose risks that may prevent them from being included in Group 1. However, experimentation and testing with permissionless blockchains by regulated financial institutions suggests that technical solutions to mitigate the risks identified by the BCBS are being actively developed and implemented. The BCBS also raises concerns with the probabilistic settlement of permissionless blockchains. However, over the last several years, market participants have been developing industry standards for determining when a settlement has completed on probabilistic blockchains. ▪ The United States should consider incorporating those standards to inform the prudential treatment of those characteristics of distributed ledger technology.		FRB, FDIC, OCC
Review the calibration of capital requirements for credit risk, market risk, operational risk, and liquidity risk to incorporate empirical evidence of recent changes in cryptoasset performance and risk. ▪ Changes in the grouping of cryptoassets may not fully modernize the BCBS cryptoasset prudential standards. The United States should also revisit the calibration of the prudential standards to consider incorporating recent innovations and changes in the cryptoasset market since the BCBS standards were first published in 2022. ▪ The Banking Agencies should undertake a comprehensive data analysis on the performance and risk of cryptoassets informed by issuing a request for information from the public, inclusive of representatives from cryptoasset data vendors, distributed ledger infrastructure providers, banking organizations of all sizes, and industry associations. The analysis would assist the Banking Agencies in determining the appropriate calibration for cryptoasset capital and liquidity standards.		FRB, FDIC, OCC

Insurance		
Recommendation	Policy Responsibility	
	Congress	Regulator
Engage with the appropriate regulatory agencies to establish or amend legal definitions of securities, property, or currency so that insurance policies explicitly cover digital assets. Treasury could also work with the insurance sector to create standardized terms, conditions, and policy language for digital assets.		Treasury
Engage with the NAIC and state insurance regulators on potential revisions to state regulations relating to digital assets, including allowing insurers to invest in digital assets, as appropriate.		Treasury
Prioritize engagement between the public and private sector to help develop a robust insurance market for digital assets.		Treasury

Stablecoins and Payments		
Recommendation	Policy Responsibility	
	Congress	Regulator
Innovation in Payments		
Faithfully and expeditiously implement GENIUS.		Primary Responsibility: Treasury, FRB, FDIC, OCC, NCUA Secondary Responsibility: SEC, CFTC
Central Bank Digital Currencies (CBDCs)		
Discourage, oppose, and prohibit the ability of any agency from undertaking any action to establish, issue, or promote any CBDCs in the United States or abroad.		Primary Responsibility: FRB, Treasury Secondary Responsibility: FDIC, OCC, NCUA
Support legislation prohibiting the adoption of any CBDCs in the United States, including, for example, the Anti-CBDC Surveillance State Act, which was passed by the House of Representatives on July 17, 2025.	Congress	
Support U.S. technological leadership and competitiveness in capital markets and work to upgrade domestic payment systems, FMIs, and cross-border payments; urge other countries to adopt policies that promote the role of the private sector within a technology-neutral regulatory regime.		Treasury, FRB, FDIC, OCC, NCUA
Examine the extent to which U.S. federal agencies (including the Banking Agencies) and relevant international financial institutions have engaged in CBDC research or pilot programs contrary to the policies set forth in Executive Order No. 14178.		Primary Responsibility: FRB, Treasury Secondary Responsibility: FDIC, OCC, NCUA

Stablecoins and Payments		
Recommendation	Policy Responsibility	
	Congress	Regulator
Promoting the Competitiveness of the U.S. Dollar		
Relevant U.S. agencies, including Treasury, should promote U.S. private sector leadership in the responsible development of innovative cross-border payments and financial markets technologies. Toward this end, Treasury should consider using its convening authority to encourage and provide clarity to U.S. financial institutions in leading these efforts.		Treasury, FRB, FDIC, OCC, NCUA
Treasury and other relevant agencies should 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. Standards, including international standards, should be calibrated to accurately reflect the risk of innovative digital products and services.		Primary Responsibility: Treasury, FRB Secondary Responsibility: FDIC, OCC, NCUA
Domestically and internationally, U.S. authorities should encourage payment solutions that: (i) protect the two-tier banking system and promote the private sector's role in financial intermediation, payments, and capital formation; (ii) preserve individual rights and limit government control of personal financial information; and (iii) incorporate robust and effective AML/CFT and sanctions controls.		Primary Responsibility: Treasury, FRB, OCC Secondary Responsibility: FDIC, NCUA
Treasury, in coordination with other relevant agencies, should engage with international counterparts and institutions by leading initiatives to upgrade domestic payment systems, FMIs, and cross-border payment systems, to help protect the primacy of the dollar-based international monetary system.		Primary Responsibility: Treasury, FRB Secondary Responsibility: FDIC, OCC, NCUA

Countering Illicit Finance		
Recommendation	Policy Responsibility	
	Congress	Regulator
Improving the AML/CFT and Sanctions Frameworks		
Prescribing BSA Obligations		
Treasury should faithfully and expeditiously implement the Guiding and Establishing National Innovation for U.S. Stablecoins Act (GENIUS), which, among other things, requires Treasury to adopt rules to treat permitted payment stablecoin issuers as financial institutions under the BSA and to seek public comment and conduct research to identify innovative or novel methods, techniques, or strategies that regulated financial institutions use to detect illicit activity involving digital assets.		Treasury

Countering Illicit Finance		
Recommendation	**Policy Responsibility**	
	Congress	**Regulator**
Digital asset market structure legislation should consider creating digital asset specific financial institution types or sub-types within the BSA. Now that GENIUS has been enacted into law, and pending additional market structure legislation being considered by Congress, 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.		Treasury
▪ 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.		
Legislation should consider specifying actors within the decentralized finance ecosystem that should have AML/CFT obligations, taking into consideration those actors' roles in the ecosystem and attendant risks.	Congress	
Treasury should consider next steps regarding its proposed rulemaking concerning CVC mixing.		Treasury
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.	Congress	
Congress should evaluate the self-custody language that is included in CLARITY and codify the following principles through legislation that reinforce the importance of self-custody:	Congress	
▪ *Principle 1*: The importance of U.S. individuals maintaining the capability to lawfully hold, or custody, their own digital assets without a financial intermediary. ▪ *Principle 2*: The importance of enabling U.S. individuals to engage in lawful, direct digital asset transfers that do not involve a financial intermediary with another individual that lawfully self-custodies digital assets.		
Congress should codify principles regarding how control over an asset impacts BSA obligations, particularly for money transmitters, through legislation such as the Blockchain Regulatory Certainty Act, which has been incorporated into CLARITY.	Congress	
▪ Specifically, such legislation could codify that a software provider that does not maintain total independent control over value is not engaged in money transmission for purposes of the BSA.		
Enhancing Effective Supervision		
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.		Treasury, FRB, FDIC, OCC, NCUA, SEC, CFTC, FHFA
Supervisors should evaluate whether additional compliance tools, training, and internal resources are needed to ensure examiners can effectively and efficiently evaluate institutions' digital asset-related policies, procedures, and programs.		Treasury, FRB, FDIC, OCC, NCUA, SEC, CFTC, FHFA

Countering Illicit Finance		
Recommendation	Policy Responsibility	
	Congress	Regulator
Adapting BSA Reporting to Better Account for Digital Assets		
Treasury should continue to evaluate modernizing Suspicious Activity Report (SAR) reporting, including the SAR form itself, to ensure it captures highly useful information.		Treasury
Congress should, through appropriate legislation, ensure that the information required by statute to be reported to FinCEN for BSA purposes under 31 U.S.C. § 5331 conforms with the information required to be reported by statute to the IRS for federal income tax purposes under 26 U.S.C. § 6050I, as was the case prior to 2021.	Congress	
Improving Sanctions Compliance with Regard to Digital Assets		
Treasury should issue a Request for Information (RFI) to directly solicit sanctions compliance information, input, and recommendations from industry participants to understand ongoing developments and innovations and gaps in existing OFAC guidance as well as to identify opportunities for enhanced private sector collaboration.		Treasury
Treasury should consider revising and updating OFAC's existing *Sanctions Compliance Guidance for the Virtual Currency Industry* brochure, which highlights existing compliance tools such as traditional sanctions screening and blockchain analytics to help improve sanctions compliance by all industry participants, in accordance with insight gleaned from the RFI process.		Treasury
Equipping Digital Asset Actors to Mitigate Risk		
Enabling Private Sector Investigations		
Congress should consider enacting a digital asset-specific "hold law" that offers a safe harbor to institutions that temporarily and voluntarily hold property involved in suspected illegal activity during a short duration investigation. Such a law should consider transparency when an asset is frozen and consumer protection measures.	Congress	
Increasing Public-Private Cooperation		
Treasury should undertake efforts to encourage greater information sharing, including through FinCEN's 314(a) and 314(b) programs. Such efforts should include encouraging domestic and cross-border information sharing, greater participation in sharing programs by digital asset financial institutions and improved information sharing between digital asset and traditional financial institutions.		Treasury
Public and private sector participation in real-time information sharing through IVAN should be encouraged to the extent consistent with legal obligations.		Treasury, DOJ, SEC, CFTC, FRB, FDIC, OCC

Countering Illicit Finance		
Recommendation	Policy Responsibility	
	Congress	Regulator
Disrupting and Mitigating Systemic Illicit Finance Risks		
Applying Treasury Authorities to Digital Asset Ecosystem		
Congress should, consistent with how it has approached Fentanyl and Russian illicit finance, add a sixth special measure to Section 311 authorizing FinCEN to prohibit, or impose conditions upon, certain "transmittals of funds" that are not tied to a correspondent banking relationship. This would enable Treasury to target foreign digital asset exchanges or digital asset transactions involving criminal or state actors—without regard to the nature of their illicit activity.	Congress	
Treasury should continue to use OFAC's sanctions authorities, which range from applying full blocking sanctions to more calibrated restrictions, to target malicious actors seeking to harm Americans and to limit the access of foreign digital asset actors engaged in illicit activity to U.S. markets, in support of the Trump Administration's priorities.		Treasury
Tailoring Law Enforcement Capabilities and Authorities		
Congress should evaluate victim compensation regulations and propose amendments to address concerns regarding victim compensation and improve asset-forfeiture efforts in the digital assets space.	Congress	
Congress should tailor 18 U.S.C. § 1014 to protect all financial institutions (defined under Title 31 of the U.S. Code), including those offering digital asset services. In addition, Congress should clarify that the law applies to all false statements in connection with obtaining or maintaining access to services from financial institutions. Relatedly, U.S.S.G. Section 2B1.1 should be updated to include a sentencing enhancement for making false statements to financial institutions where the scheme involves significant volume of criminal funds but no loss to the institution.	Congress	
Congress should amend the NSPA to clarify that digital assets are property subject to this act.	Congress	
Congress should amend the anti-tip-off provision in 18 U.S.C. § 1510 to update the definition of "financial institution" from the narrower definition found in 18 U.S.C. § 20 to the broader definition found in the BSA, 31 U.S.C. §§ 5312(a)(2) and (c), to cover, among other additions, certain digital asset firms that operate as money services businesses (MSBs). Congress should also amend the same anti-tip-off provision to include additional serious underlying offenses as covered offenses to prohibit agents of financial institutions from tipping off suspects.	Congress	
Congress should amend 18 U.S.C. § 984 to make certain digital assets subject to the same modified traceability requirement as exists for cash to allow the government to seize and forfeit digital assets found in the same wallet used to hold crime-linked digital assets, without requiring the government to prove the forfeited assets were the exact same digital assets derived from or used to commit a criminal offense.	Congress	

Countering Illicit Finance		
Recommendation	Policy Responsibility	
	Congress	Regulator
Advancing Privacy through Digital Identity and Related Tools		
Treasury should consider coordinating with the National Institute of Standards and Technology (NIST), and other federal agency partners as appropriate, to: ▪ Identify emerging approaches to implement customer identification in digital asset scenarios, including possible applications of the Fourth Revision of the NIST Digital Identity Guidelines (SP 800-63-4) to these scenarios. ▪ Evaluate lessons learned in the project "Accelerate Adoption of Digital Identities on Mobile Devices" being executed in the National Cybersecurity Center of Excellence for applicability to customer identification programs in digital asset scenarios. ▪ Evaluate the digital asset ecosystem, including existing identity credentialing tools and technical aspects of digital asset services, to determine potential approaches for defining, mandating, and enforcing customer identification programs and evaluate the potential efficacy of such schemes in detecting, deterring, and investigating fraudulent transactions.		Treasury, Commerce
As is required by GENIUS, Treasury should issue an RFI to gather information on innovative tools to detect illicit activity, including with respect to digital identity verification.		Treasury
Treasury should, in consultation with the federal functional regulators, consider issuing guidance to financial institutions on how they can utilize digital identity solutions within their existing customer identification programs. Treasury should ensure that future guidance balances secure identity verifications with protection of personally identifiable information.		Treasury, SEC, CFTC, FDIC, OCC, FRB, NCUA

Taxation		
Recommendation	Policy Responsibility	
	Congress	Regulator
Substantive Tax Issues		
Treasury and the IRS should publish guidance addressing the determination of "adjusted financial statement income" (AFSI) with respect to financial accounting unrealized gains and losses on investment assets other than stock and partnership interests. Toward this end, the IRS issued Notice 2025-27 stating that Treasury and the IRS anticipate interim guidance under CAMT to address how unrealized gains and losses on certain investment assets reported for financial statement purposes are considered for purposes of determining AFSI.		Treasury, IRS
Treasury and the IRS should publish guidance addressing whether a trust that otherwise qualifies as an investment trust treated as a grantor trust fails to qualify as such if the trust stakes digital assets owned by the trust.		Treasury, IRS
Treasury and the IRS should publish guidance addressing whether wrapping and unwrapping transactions are taxable transactions.		Treasury, IRS
Treasury and the IRS should update the IRS FAQs on digital assets.		Treasury, IRS

Taxation		
Recommendation	Policy Responsibility	
	Congress	Regulator
Legislation should be enacted that 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. Code provisions that should be expanded to apply to actively traded fungible digital assets include Sections 475 (mark-to-market election), 864(b) (trading safe harbors), 1058 (securities loans), and 7704 (publicly traded partnership rules). In addition, Sections 1091 (wash sale rules) and 1259 (constructive sales) also should apply to digital assets. Alternatively, legislation could instead clarify when a digital asset commodity or other digital asset is treated as a security or a commodity for federal income tax purposes.	Congress	
Legislation should be enacted that would characterize payment stablecoins for federal income tax purposes, as such matters are not addressed by GENIUS. If payment stablecoins are treated as debt, legislation should consider the applicability of existing federal income tax rules that could impede the widespread use of payment stablecoins as financial assets that function in a similar manner to cash-equivalents. In particular, legislation should address the wash sale and anti-bearer bond rules. To address the wash sale rules, possible options include: ▪ Providing that the wash sale rules do not apply to payment stablecoins; ▪ Providing that the wash sale rules do not apply to de minimis losses from payment stablecoins, possibly up to an aggregate threshold; or ▪ Providing that gains and losses on payment stablecoins are not considered for federal income tax purposes. If no such legislation is enacted, Treasury and the IRS should consider issuing guidance that would clarify the tax classification of payment stablecoins, and address the potential application of the wash sale and anti-bearer bond rules.	Congress	Treasury, IRS
The wash sale rules should be amended to add digital assets to the list of assets subject to the wash sale rules. If legislation of this kind is enacted, the broker reporting regulations should be amended to reflect these changes to the wash sale rules. Further, the wash sale rules should not apply to payment stablecoins.	Congress	
Legislation should be enacted to amend Section 1058 to provide that it applies to loans of actively traded fungible digital assets, provided that the loan has terms similar to those currently required for loans of securities. The Secretary of the Treasury should be granted authority to determine when a digital asset is actively traded, and to address differences between the standard terms of securities loans and crypto loans.	Congress	Treasury
Taxpayer Reporting		
Treasury and the IRS should issue administrative guidance that addresses de minimis receipts of digital assets. The guidance could apply to airdrops, staking, hard forks, and mining rewards for taxpayers who do not operate a node or carry out digital asset mining.		Treasury, IRS
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, taking into account any recent intervening developments since the issuance of such guidance.		Treasury, IRS
If Congress decides to pass legislation regarding the timing of the inclusion of income relating to mining or staking, Congress should consider whether similar rules should apply to rewards from other digital asset validation methods, what the character of income upon disposition should be and if ordinary, what rules should apply to determine the order of dispositions of ordinary versus capital units, and potential differences between the fair market value of rewards at the time of receipt compared with the fair market value of rewards at the time of sale or other disposition.	Congress	

Taxation		
Recommendation	Policy Responsibility	
	Congress	Regulator
Legislation could be enacted that would require taxpayers to report foreign digital asset accounts. A foreign digital asset account would be a custodial account that holds digital assets that is maintained by a foreign digital asset exchange or other foreign digital asset service provider. If the United States implements the Crypto-Asset Reporting Framework (CARF), taxpayers could be required to report accounts with foreign crypto-asset service providers that are required to report information on U.S. customers to a non-U.S. tax authority.	Congress	
Legislation could be enacted that would streamline the reporting required under Section 6038D and on the FBAR. Legislation could permit a taxpayer that is subject to both reporting obligations to submit a single form that would be available both to the IRS and to FinCEN.	Congress	
Third-Party Information Reporting		
Treasury and the IRS should propose regulations that provide brokers that facilitate sales or exchanges of digital assets through electronic means with a less burdensome method of obtaining consent from their customers to furnish Form 1099-DA payee statements in an electronic format.		Treasury, IRS
Treasury should consider proposing regulations to implement CARF that take stakeholder concerns into account and minimize burdens on brokers to the extent consistent with CARF rules. The proposed regulations should not impose any new reporting requirements on DeFi transactions and should be used as a forum to gather further feedback, including a reasonable timetable for CARF implementation.		Treasury, IRS
Treasury and the IRS should consider proposing regulations requiring basis information to be reported when digital assets are transferred between centralized digital asset exchanges.		Treasury, IRS
Treasury and the IRS should consider proposing regulations implementing reporting of digital assets paid to a trade or business in a manner that takes stakeholder concerns into account.		Treasury, IRS
Consideration should be given to legislation to conform the information required to be reported to FinCEN, for BSA purposes, and the IRS, for federal income tax purposes. The legislation could also reexamine the reporting dollar thresholds and the breadth of uses of digital assets to which this provision would apply.	Congress	

Miscellaneous Recommendations		
Recommendation	Policy Responsibility	
	Congress	Regulator
Cybersecurity		
The Working Group recommends that relevant agencies develop principles-based requirements and standards, as appropriate, for digital asset firms. Such principles-based requirements and standards should take into account the various activities and related risks of various industry participants to strengthen industry's protection from malicious cyber actors.		Treasury, SEC, CFTC, FRB, FDIC, OCC, NCUA
The Working Group recommends that relevant agencies consider measures to increase information sharing on potential threats across the private sector and between the public and private sectors.		Treasury, SEC, CFTC, FRB, FDIC, OCC, NCUA
Treasury's OCCIP could work with industry to identify opportunities to increase information sharing on cybersecurity risks, including by providing U.S. regulated digital asset firms access to the ATIF.		Treasury
Treasury's OCCIP—through the existing public-private partnership structure—could explore identifying gaps in addressing operational resiliency of digital asset firms to enable broader adoption.		Treasury
Repatriation and Domestication of Offshore Foundations		
The Working Group encourages non-profit organizations supporting the development of blockchain technologies to domicile in the United States. Toward this end, the Working Group will engage with Treasury and the IRS to study ways to incentivize their repatriation and domestication.	Congress	Working Group, Treasury, IRS

Cementing U.S. Leadership through the Bitcoin Strategic Reserve and U.S. Digital Asset Stockpile

Under President Trump's Executive Order No. 14178, the Working Group shall "evaluate the potential creation and maintenance of a national digital asset stockpile and propose criteria for establishing such a stockpile, potentially derived from cryptocurrencies lawfully seized by the U.S. Government through its law enforcement efforts."[494] On March 6, 2025, the President issued Executive Order No. 14233, which clarified and expanded on this directive and provided that it is the policy of the United States to establish a Strategic Bitcoin Reserve (the "Reserve") and a United States Digital Asset Stockpile (the "Stockpile").[495]

Consistent with the framework established by these executive orders:

- The Reserve and the Stockpile will be administered by Treasury, which will establish an office to administer and maintain control of the associated custodial accounts
- The Reserve and the Stockpile will be capitalized by forfeited digital assets—in other words, digital assets owned by the U.S. government.
- However, forfeited digital assets needed to satisfy statutory objectives will continue to be used for those objectives, including to compensate identifiable and verifiable victims of crimes, to support law enforcement operations, to be equitably shared with state and local law enforcement partners, and to fulfill other statutory forfeiture program requirements.
- The bitcoin in the Reserve will generally not be sold and will be maintained as reserve assets of the United States utilized to meet governmental objectives in accordance with applicable law.
    - Treasury and Commerce will develop strategies that could be used to acquire additional bitcoin[496] for the Reserve in ways that are budget neutral and do not impose incremental costs on United States taxpayers.
- Custody will be studied by Treasury and Commerce in order to safeguard the assets of the United States.

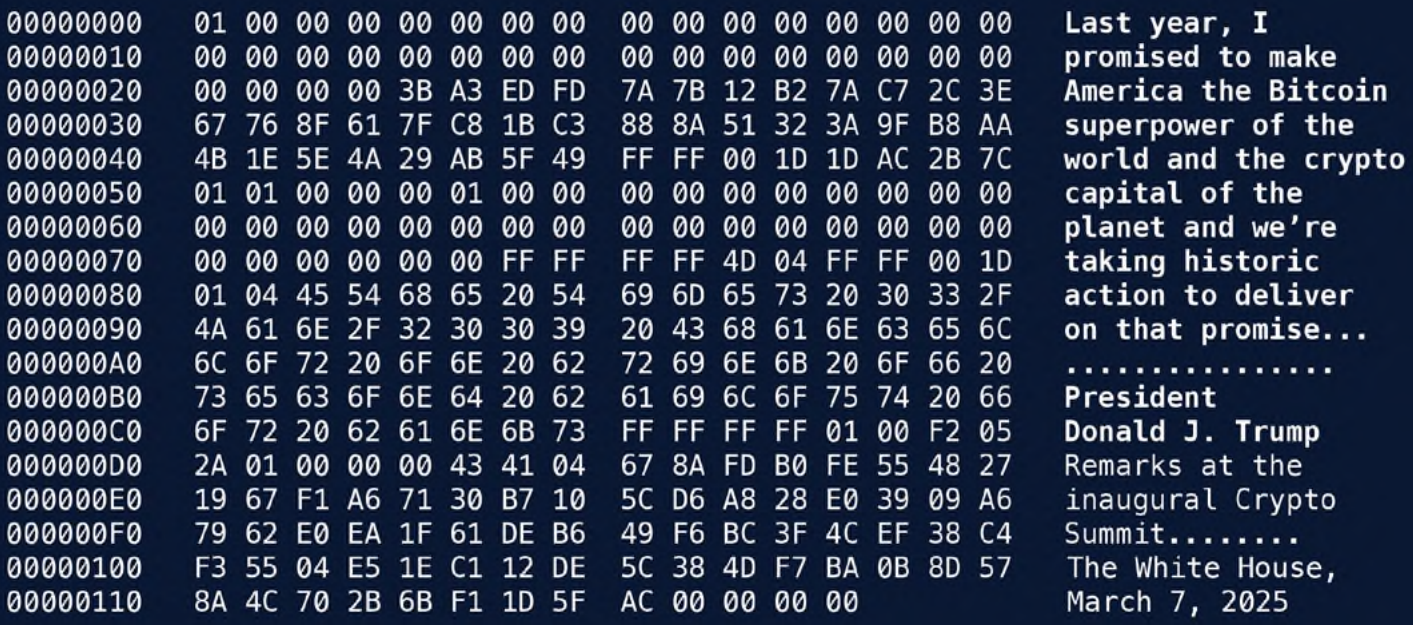
Pursuant to Section 3(e) of Executive Order No. 14233, Treasury delivered considerations to the White House regarding the establishment and management of the Reserve and the Stockpile. Treasury will continue to coordinate with the White House and other members of the Working Group to move forward with appropriate next steps to operationalize the Reserve and the Stockpile for the benefit of the United States government and taxpayers.[497]

494 Exec. Order No. 14178, *supra* note 2, at § 4(c)(2).

495 Exec. Order No. 14233, Establishment of the Strategic Bitcoin Reserve and United States Digital Asset Stockpile, 90 Fed. Reg. 11789 (Mar. 6, 2025).

496 Bitcoin enthusiasts use the phrase "stacking sats" to describe acquiring incremental amounts of bitcoin. "Sat" is short for "Satoshi," the smallest possible unit of bitcoin the network can accommodate (0.00000001 bitcoin). *See Stack the Sats Meaning,* Ledger Academy (Mar. 2024), https://www.ledger.com/academy/glossary/stack-the-sats.

497 *See* Exec. Order No. 14233, *supra* note 495, at § 3(e). *See* Exec. Order No. 14233, *supra* note 495, at § 3(e).


00000000 01 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00000010 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00000020 00 00 00 00 3B A3 ED FD 7A 7B 12 B2 7A C7 2C 3E
00000030 67 76 8F 61 7F C8 1B C3 88 8A 51 32 3A 9F B8 AA
00000040 4B 1E 5E 4A 29 AB 5F 49 FF FF 00 1D 1D AC 2B 7C
00000050 01 01 00 00 00 01 00 00 00 00 00 00 00 00 00 00
00000060 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00000070 00 00 00 00 00 00 FF FF FF FF 4D 04 FF FF 00 1D
00000080 01 04 45 54 68 65 20 54 69 6D 65 73 20 30 33 2F
00000090 4A 61 6E 2F 32 30 30 39 20 43 68 61 6E 63 65 6C
000000A0 6C 6F 72 20 6F 6E 20 62 72 69 6E 6B 20 6F 66 20
000000B0 73 65 63 6F 6E 64 20 62 61 69 6C 6F 75 74 20 66
000000C0 6F 72 20 62 61 6E 6B 73 FF FF FF FF 01 00 F2 05
000000D0 2A 01 00 00 00 43 41 04 67 8A FD B0 FE 55 48 27
000000E0 19 67 F1 A6 71 30 B7 10 5C D6 A8 28 E0 39 09 A6
000000F0 79 62 E0 EA 1F 61 DE B6 49 F6 BC 3F 4C EF 38 C4
00000100 F3 55 04 E5 1E C1 12 DE 5C 38 4D F7 BA 0B 8D 57
00000110 8A 4C 70 2B 6B F1 1D 5F AC 00 00 00 00
Last year, I promised to make America the Bitcoin superpower of the world and the crypto capital of the planet and we're taking historic action to deliver on that promise...
.....
President Donald J. Trump
Remarks at the inaugural Crypto Summit.....
The White House, March 7, 2025

THE WHITE HOUSE

WASHINGTON