Congressional Research Service
Informing the legislative debate since 1914

Cryptocurrency: Selected Policy Issues

February 15, 2023

Congressional Research Service
https://crsreports.congress.gov
R47425

CRS REPORT
Prepared for Members and
Committees of Congress

Congressional Research Service
Informing the legislative debate since 1914

SUMMARY

R47425

February 15, 2023

Paul Tierno
Analyst in Financial Economics

Cryptocurrency: Selected Policy Issues

Cryptocurrencies are digital financial instruments exchanged across public blockchains, and recorded on ledgers, that do not require central intermediaries (e.g., commercial banks, central banks) for clearing and settlement. Satoshi Nakamoto, an anonymous individual or collective, introduced the first cryptocurrency, Bitcoin, in a whitepaper in 2008 and a subsequent blockchain in 2009. While Bitcoin was a novel form of financial transaction, it built on technology that had been decades in the making, including blockchains, cryptography, and consensus protocols, among others.

Cryptocurrency (or crypto) attempts to replace the current financial system, of which a central tenet is trust, with one that does not require trust. A variety of safeguards are built into traditional banking and payments systems to foster trust and inspire confidence, including, among others, chartering procedures, capital requirements, ongoing supervision, and deposit insurance. In place of trust, the cryptocurrency system leverages a series of separate but concurrent incentives for different system participants.

Cryptocurrency was initially developed as a payments system. Cryptocurrency transactions have proven to take longer and be costlier to settle than existing payments options, creating challenges for wider adoption. Adoption challenges, combined with crypto's periodic bouts of sharp price fluctuations, have fueled crypto's use as a speculative investment.

Once used by a small subset of computer scientists, cryptocurrency has gone global. The crypto market capitalization reached a high of nearly $3 trillion in November 2021, with an estimate of more than 10,000 cryptocurrencies in circulation. This growth was both the product of and subsequent catalyst to ongoing changes in the industry. For example, crypto was originally accessible via less-than-user-friendly blockchains, but companies and applications created more user-friendly and familiar systems that allow individuals and firms to "custody" their crypto in accounts or wallets at institutions. Specifically, an entire ecosystem has developed that supports cryptocurrencies, including the custody or hosting services known as wallets, as well as exchanges, payment platforms that support crypto, decentralized finance platforms, and dozens more. In the process, large traditional financial intermediaries—the very type of institutions crypto wanted to make unnecessary—have displaced the decentralized, trustless ideal. Coincidentally, since November 2021, crypto has experienced a significant decline and lost more than $2 trillion, or greater than 70% of market value.

Currently, there is no overarching regulatory regime for crypto. Federal regulators have adapted existing regulations where cryptocurrency resembles traditional products and services in the financial sector. Regulation has generally flowed from enforcement actions rather than rulemaking, limiting the reach of regulators and creating regulatory ambiguity for the crypto industry. Federal financial regulators claim varying degrees of authority over different corners of the industry.

The novelty of cryptocurrencies' design, the brisk pace of their ascent, and the general dynamic of the crypto industry—particularly a series of crypto company failures in 2022, highlighted by the collapse of FTX, a popular exchange—point to various policy questions that may be of interest to Congress. Whether a regulatory regime that is tailored for crypto is necessary is subject to debate. The current regulatory approach has kept the industry at arm's length from the traditional financial system, a fact that has limited broader systemic risk but whose lighter touch may have enabled fraud. Chief issues in this debate are questions over how to balance the relative privacy crypto provides with its potential for use in illicit activity and whether investor protections should be put in place in an industry that has been rife with scams and thefts. Inviting crypto further into the regulatory perimeter may enhance regulation and oversight, but it may also increase systemic risk and confer on the industry a sense of legitimacy some do not believe it deserves. In addition, the industry faces criticism for its large carbon footprint.

Contents

Introduction 1
What Is Cryptocurrency? 3
Blockchain, Decentralized Consensus, and Cryptography 4
Transactions 6
An Overview of Crypto Markets 7
Cryptocurrencies 7
Bitcoin 8
Ethereum 9
Stablecoins 10
Central Bank Digital Currency 11
Ways to Interact with Crypto 12
On-Chain Transactions 12
Decentralized Finance (DeFi) 14
Off-Chain Transactions 14
Cryptocurrency Exchanges 15
Crypto on Payments Apps 16
Traditional Financial Institutions and Crypto 16
Selected Policy Issues 17
Inclusion and Scalability 17
Privacy versus Security 19
Existing Regulation of Cryptocurrency 20
Applicable SEC Framework 21
Applicable CFTC Framework 23
Applicable Bank Framework 24
Applicable Money Services Businesses Framework 25
The Future of Cryptocurrency Regulation 26
Tax Implications 28
Energy Intensity 29
Outlook 30

Figures

Figure 1. Traditional Payments 3
Figure 2. How Does a Transaction Get into the Blockchain? 6

Contacts

Author Information 30

Introduction

In January 2009, Satoshi Nakamoto—the pseudonym of an unidentified computer scientist (or collective of scientists)—mined the first block (or group of transactions) on the Bitcoin network a few months after publishing the "Bitcoin Whitepaper."[1] This *Genesis Block*—as the first transaction on the Bitcoin network was called—included an encoded message that referred to a newspaper headline published around that time: "Chancellor on brink of second bailout for banks."[2] The article the block referenced described a bailout for English banks in the immediate aftermath of the global financial crisis. While the message was relevant historical context for when the transaction occurred, transactions processed on the Bitcoin network include dates and timestamps, so the reference to the English bank bailout was unnecessary. Instead, Satoshi Nakamoto and commentators have since clarified that this allusion to banking conditions was intended to draw a contrast between the new financial paradigm Bitcoin represented and the traditional financial system.[3] These early developers did not want to rely on a financial system dependent on third parties—especially governments and central and commercial banks—but instead created a system to bypass them.

Cryptocurrency's initial use case was as a combined payment system and unit of account that eschewed intermediaries. Traditional payments systems are composed of various banks, payments processors, credit card networks, central clearinghouses, central banks, and a vast technological infrastructure that supports it. In this system, banks ultimately validate customer transactions and log the details of the transactions digitally in their private ledgers. Banks then submit these details via messaging networks, which authorize transactions to occur, and ultimately facilitate the exchange of funds at banks' master accounts at a national central bank, which in the United States is the Federal Reserve. As such, transactions between two individuals with accounts at two or more different financial institutions involve at least two commercial bank ledgers and the ledger of at least one central party, which acts as an intermediating agent for the transacting parties. (See **Figure 1** for a simplified version of transactions.) In addition to this massive infrastructure, the system requires trust and security, which safeguards deposits regardless of economic conditions. It requires that banks perform their responsibilities effectively and maintain effective risk management controls, including over their payments systems. Moreover, it obligates banks to do their best to safeguard their data and extend services to qualifying customers.

Cryptocurrency, on the other hand, is a payment and value storage system that functions as "electronic cash protected through cryptographic mechanisms instead of a central repository or authority."[4] In lieu of independent financial institutions with individual ledgers relying on third-

[1] For information on the Genesis Block, see Brenden Rearick, "What Is the Genesis Block? 8 Things to Know as Investors Celebrate 'Bitcoin's Birthday,'" *Yahoo*, January 3, 2022, https://www.yahoo.com/now/genesis-block-8-things-know-215101010.html. Satoshi Nakamoto, "Bitcoin: A Peer-to-Peer Electronic Cash System," October 10, 2008, https://Bitcoin.org/Bitcoin.pdf.

[2] The headline is from a story published in *The Times* on January 3, 2009. See this article at Bryce Elder, "Happy Birthday to a Giant Ponzi Scheme,' from Bitcoin's Accidental Co-Creator," *Financial Times*, January 3, 2023, https://www.ft.com/content/465fb224-3fc9-4b37-81d4-39eece1041df.

[3] Pymnts, "A Bitcoin Declaration of Financial Independence," July 4, 2022, https://www.pymnts.com/blockchain/Bitcoin/2022/a-Bitcoin-declaration-of-financial-independence/. See http://p2pfoundation.ning.com/forum/topics/Bitcoin-open-source?id=2003008%3ATopic%3A9402&page=1 for a blog post attributed to Satoshi Nakamoto on the role of central banks in the past.

[4] Dylan Yaga et al., *Blockchain Technology Overview*, National Institute of Standards and Technology, October 2018, p. iv, https://nvlpubs.nist.gov/nistpubs/ir/2018/NIST.IR.8202.pdf.

party mediation and securing consumer trust, the crypto system consists of a single ledger distributed to all members of the network that is constantly updated. Users believe the system works because they can see it and track it. The system uses cryptography and incentives for diverse participants to secure the network.

Since 2009, the crypto industry—which now consists of thousands of cryptocurrencies and various applications—has experienced both relatively low adoption as a payment tool and various periods of rapid price increases and decreases. These two facets combined have helped fuel crypto as a speculative asset at the expense of its use as a payment tool. In this context, crypto became a victim of its own success. Using crypto for routine payments was not attractive when holding it could yield significant return.[5] Its novelty and opaqueness and the mystery behind its origins sustain a lore that boosted cryptocurrency's popularity.

At the same time, the industry is rife with ideological tensions that have become more visible since the market lost more than 70% of its peak market capitalization and some of its most visible companies—including FTX, which at its peak had been the third-largest crypto exchange—collapsed.[6]

Some say the industry is a technological solution in search of a problem. Some who espouse this view note that the technology and industry as a whole do not have an economic or productive capacity beyond speculation or the expectation of appreciation.[7] Moreover, if there is no productive use for crypto, then its large carbon emissions and energy use appear more problematic, according to this view. The Bitcoin network alone, for example, uses as much energy and produces emissions comparable to nation states.[8] Proponents of crypto disagree, believing that it is a new and innovative technology with potentially valuable and paradigm-shifting applications, many of which may not yet be realized. Internally, the recent and relentless failure of centralized crypto institutions highlights the tension between (1) factions that adhere to the idealistic origins of decentralization and (2) the institutions that have fueled its trajectory from obscure technology to financial mainstay.

The rise of cryptocurrencies has produced a host of policy issues that may be of interest to Congress. In light of crypto's various potential use cases and factions (e.g., payments vs. speculative investment, decentralized vs. centralized), crypto has become a Rorschach test of sorts in which users and policymakers see in it what they value most and interpret policy considerations through that same lens. The host of policy issues raised includes, among others: managing the tension between public interest in privacy and government desire to monitor and eliminate illicit financial activity, the ongoing debate on the adequacy of the existing regulatory structure, determining whether cryptocurrencies should be considered currencies or property for tax purposes, and the industry's potential contribution to climate change.

---

[5] For a discussion of the conceptual foundation of cryptocurrency, see CRS Report R45427, *Cryptocurrency: The Economics of Money and Selected Policy Issues*, by David W. Perkins.

[6] Associated Press, "The Downfall of FTX's Sam Bankman-Fried Sends Shockwaves Through the Crypto World," November 14, 2022, https://www.npr.org/2022/11/14/1136482889/ftx-sam-bankman-fried-shockwaves-crypto.

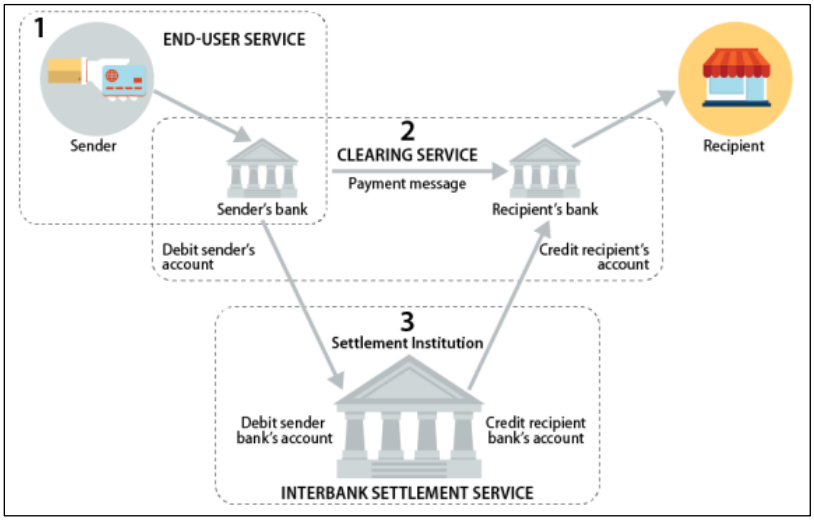
[7] See, for example, Joe Weisenthal and Tracy Alloway, "Aaron Lammer on Yield Farming and Trading in the World of DeFi," *Bloomberg Odd Lots (Podcast)*, May 22, 2021, at 43:00, https://podcasts.apple.com/us/podcast/aaron-lammer-on-yield-farming-and-trading-in-the/id1056200096?i=1000522481080; and Hilary Allen, "The Superficial Allure of Crypto," *IMF Finance and Development*, September 2022, https://www.imf.org/en/Publications/fandd/issues/2022/09/Point-of-View-the-superficial-allure-of-crypto-Hilary-Allen.

[8] For comparison and other Bitcoin-related energy statistics, see the Cambridge Bitcoin Electricity Index at https://ccaf.io/cbeci/ghg/comparisons.

In March 2022, the Biden Administration issued Executive Order 14067 on Ensuring Responsible Development of Digital Assets acknowledging these various policy implications, with the stated objectives of protecting consumers, ensuring American and global financial stability, preventing illicit financial activity, and promoting access to affordable financial resources.[9]

This report provides an overview of cryptocurrency, including the technology behind it. It examines the different ways users can participate in the market—distinguishing on-chain decentralized transactions from centralized off-chain transactions and the entities providing these services. It provides an overview of some of the key assets that make up the market. Finally, it examines policy issues, including, among others, how the existing regulatory frameworks treat cryptocurrencies and its various functions.

Figure 1. Traditional Payments



Source: Federal Reserve, "Potential Federal Reserve Actions to Support Interbank Settlement of Faster Payments," 83 *Federal Register* 221, November 15, 2018, p. 57356, https://www.govinfo.gov/content/pkg/FR-2018-11-15/pdf/2018-24667.pdf.

Note: See text for details.

What Is Cryptocurrency?

Cryptocurrencies consist of both the units of stored value and the networks on which they are exchanged. The cryptocurrencies discussed in this report are decentralized and permission-less, which means that neither a transacting participant nor a *node*, which is a component that supports the system in some capacity, requires any permission or special authorization to participate in the network or modify the ledger of transactions.[10] (Some of the system-supporting participant *nodes* are called *validators* or *miners*.) Cryptocurrency networks are comprised of unaffiliated participants operating specific software that they have downloaded on individual computers—not a central server. These key features distinguish the technology from traditional bank ledger

[9] Executive Order 14067, "Executive Order on Ensuring Responsible Development of Digital Assets," https://www.whitehouse.gov/briefing-room/presidential-actions/2022/03/09/executive-order-on-ensuring-responsible-development-of-digital-assets/.

[10] Cryptocurrencies may also be permissioned. See CRS Report R47064, *Blockchain: Novel Provenance Applications*, by Kristen E. Busch, for an explanation of the difference between permissioned and permission-less blockchains.

management, which requires specific permissions to access accounts as well as to implement and approve transactions.

There are countless components to the underlying technology. This section provides a limited overview of some of the primary technical components—namely, cryptographic protocols, consensus mechanisms, and transaction details. These components were chosen because they are useful to provide a cursory review of how the system works.[11]

Blockchain, Decentralized Consensus, and Cryptography[12]

Cryptocurrency is built on blockchain technology. The blockchain is a type of database that—in its application in cryptocurrencies—operates as a ledger, recording the various transactions of its participants. In the context of cryptocurrency, transactions are grouped together in *blocks* and, once approved, added to the chain of previously approved blocks. According to a National Institute of Standards and Technology report, blockchains "enable a community of users to record transactions in a shared ledger within that community, such that under normal operation of the blockchain network no transaction can be changed once published."[13] Computer scientists define *blockchains* thus as *append-only*, which means once published they can be added to but not otherwise amended. This append-only nature of blockchains, also often referred to as *immutability*, is crucial because system participants, including network nodes and miners, can identify attempted tampering.

The fact that blockchains are shared and immutable allows there to be no central intermediary responsible for approving transactions or confirming their veracity before they are added to the blockchain. There is also not a central body that approves which entities *may* approve transactions. Cryptocurrencies instead rely on what is commonly referred to as *decentralized consensus model*, in which many network participants (referred to as *mining* or *validator* nodes) compete with each other to authorize blocks of transactions for the promise of compensation (a *block reward)*, usually in currency native to a specific network or blockchain.

Cryptocurrency Mining

Mining is the process whereby certain nodes in the network (called *miners)* validate blocks of transactions, thereby adding blocks to the blockchain and updating the distributed ledger. The work of miners is described as generating random numbers that meet certain parameters. This process is called *hashing*. Hashing converts large amounts of data—the details of various transactions—into unique, fixed-length alphanumeric outputs, from which it is impossible to retrieve the original inputs. For example, the hashing program can *hash* just one word or an entire book, and in each case, the product will be a different alphanumeric value of the same length. Just knowing the output would give no additional information about the data (the word or the book from this example) added to the block.

Miners use computers to find this fixed-length standard numerical figure by combining transaction data from the current block, the previous block's hash, and a nonce. (A nonce is some random number—essentially a guess—needed to find a hash.)[14]

[11] For more on the technology behind cryptocurrency, see CRS Report R45116, *Blockchain: Background and Policy Issues*, by Chris Jaikaran; and CRS Report R47064, *Blockchain: Novel Provenance Applications*, by Kristen Busch.

[12] This section includes only a sampling of the technical components of some cryptocurrencies, including Bitcoin. This list and description is not intended to be exhaustive.

[13] Yaga et al., *Blockchain Technology Overview*, p. iv.

[14] Yaga et al., *Blockchain Technology Overview*, p. 9.

Different cryptocurrencies may have different criteria. But in the *proof of work* consensus mechanisms, the hash must meet certain parameters for the block to be added to the chain. Namely, a certain number of leading zeros must precede it. Because miners use a standard program—which creates a random hash from the block data, previous hash, and nonce—miners cannot control the output they generate when hashing and must continue the process each time using different nonces until one miner achieves a random hash that meets the difficulty requirement. (Each time a hash is attempted, computers create a random 64-digit alphanumeric string of characters. The level of difficulty of finding a correct random output increases with the requisite number of preceding zeros.[15]) The miner that generates a suitable hash is awarded a block reward. Then the system sets about it all over again, mining the next block. Generating hashes quickly requires significant computational power, energy consumption, and increasingly specialized and expensive equipment.

While being the first to generate the hash is difficult, validating that the solution is correct is easy. Moreover, because data from the preceding block is used as an input for hashing the subsequent block, tampering with any previous block—in effect attempting to change the ledger of who owns what—would show in subsequent blocks.[16] All participants would be aware if a miner retroactively tries to change a previous block (or mines a block with a transaction that tries to do so). Typically, miners want only to mine on top of blocks that have been appropriately mined. Herein lies the mechanism that allows disparate nodes that do not know each other to form a consensus.[17] Miners would not want to add subsequent blocks to a bad block out of fear that that path of the chain will be abandoned, a new strand of the chain created, and the cryptocurrency held on the old strand of blocks—called a fork—deemed worthless.[18]

The second cryptographic function that secures blockchain-based transactions is asymmetric-key cryptography, sometimes referred to as public key cryptography. Asymmetric-key cryptography uses two keys—private and public—to secure verification of a transaction. System participants use the public key to encrypt the data and, as the name suggests, can publish it and make it widely available. Encrypted messages can then be sent on to their recipients and may be decrypted only by the private key, which is (or should be) kept secret.[19]

---

[15] Anders Brownworth, "How Blockchain Works, Blockchain 101—A Visual Demo," http://blockchain.mit.edu/how-blockchain-works. For difficulty of generating preceding zeroes, see Vitalik Buterin, "What Proof of Stake Is and Why It Matters," *Bitcoin Magazine*, August 26, 2013, https://Bitcoinmagazine.com/culture/what-proof-of-stake-is-and-why-it-matters-1377531463.

[16] Brownworth, "How Blockchain Works." To illustrate, this paragraph may be hashed to produce a hash output. Moreover, data created from the hash is used as an input for transaction data in the next block, and any tampering to a previous block would show in subsequent ones. If even one character were changed and the paragraph rehashed, the function would produce an entirely different hash, making the edits immediately obvious, akin to a word processing version of track changes.

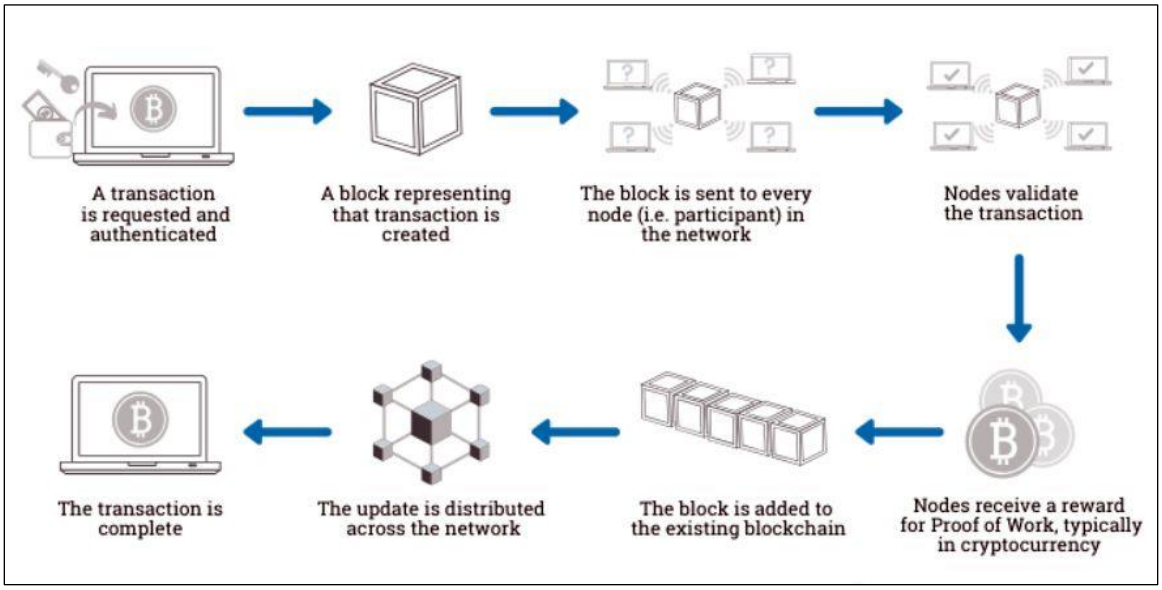
[17] Yaga et al., *Blockchain Technology Overview*, p. 18.

[18] This is commonly referred to as the Byzantine Generals problem. For more on the Byzantine Generals Problem, see Leslie Lamport, Robert Shostak, and Marshall Pease, "The Byzantine Generals Problem," *ACM Transactions on Programming Languages and Systems*, vol. 4, no. 3 (July 1982), pp. 382-340, https://www.microsoft.com/en-us/research/uploads/prod/2016/12/The-Byzantine-Generals-Problem.pdf.

[19] See CRS Report R44642, *Encryption: Frequently Asked Questions*, by Chris Jaikaran, and Yaga et al., *Blockchain Technology Overview*, p. 11. According to the National Institute of Standards and Technology, "One can encrypt with a private key and then decrypt with the public key. Alternately, one can encrypt with a public key and then decrypt with a private key" (Yaga, et al., *Blockchain Technology Overview*, p. 11).

Participants use private keys to digitally sign transactions. The authenticity of private keys is verified with the public key.[20] Importantly, it is infeasible to ascertain the private key from the available public key, therefore allowing users to share public keys. When executing transactions, individuals use private keys to digitally sign transactions such that a recipient can use the associated public key to confirm the authenticity of the sender.[21]

Figure 2. How Does a Transaction Get into the Blockchain?



Source: Euromoney Learning, https://www.euromoney.com/learning/blockchain-explained/how-transactions-get-into-the-blockchain.

Transactions

Conceptually, currencies can be token-based or account-based. In token-based currencies, assets must be verified or proven to be genuine. By contrast, account-based systems require user identification verification.[22] The quintessential token-based system, for example, is a physical currency, where the primary concern is that the bill or coin is genuine. In account-based systems, individuals and institutions must verify their identities and follow protocol, which allows them to facilitate transactions for accounts held at financial institutions.[23]

Crypto (and in particular Bitcoin) has been described as both account-based and token-based. First, it follows the definition of *account-based* because only a private key holder can access and transact with crypto associated with a blockchain address, with the private key validating the user. Bitcoin also fits the definition of *token-based*. The transaction history as recorded in the ledger

[20] Yaga, et al., *Blockchain Technology Overview*, p. 11.

[21] See CRS Report R45116, *Blockchain: Background and Policy Issues*, by Chris Jaikaran; Gary Gensler, "Blockchain and Money," Massachusetts Institute of Technoloby, 2018, at 55:20, https://www.youtube.com/watch?v=0UvVOMZqpEA; and Yaga et al., *Blockchain Technology Overview*, p. 11.

[22] For a conversation about token- and account-based systems, see Rod Garratt, Michael Lee, and Brendan Malone, "Token- or Account-Based? A Digital Currency Can Be Both," Federal Reserve Bank of New York, August 12, 2020, https://libertystreeteconomics.newyorkfed.org/2020/08/token-or-account-based-a-digital-currency-can-be-both/.

[23] Garratt, Lee, and Malone, "Token- or Account-Based?"

verifies that a unit or token (referred to as unused transaction output or UTXO) has not been spent, is in essence valid, and may be transacted.[24]

Blockchain-based systems typically require and generate two pieces of transaction data: inputs and outputs. In the case of blockchain-based cryptocurrency, this comprises transaction data. Inputs are a list of "digital assets to be transferred" with proof of provenance, such as the previous transaction (where a sender received the assets or an origin event, where new funds were created).[25] The outputs are the new assignments of ownership of input funds. For example, if Alice wants to pay Bob $17 worth of Bitcoin, a possible input would be $20 with outputs of $17 assigned to Alice and $3 assigned as "change" back to Alice. That $3 may be used on its own or with other unspent transactions to fuel another transaction.[26]

In sum, individuals who want to acquire a particular cryptocurrency for transactions (or speculative purposes) can do so by becoming nodes on the network. (Alternatively, individuals can purchase on centralized exchanges, as discussed in "Cryptocurrency Exchanges" below). In transactions, a user accesses unspent funds with a private key and sends those funds to another user on the same network.

An Overview of Crypto Markets

Cryptocurrencies may be used to facilitate transactions and may be held as speculative investments. Since 2009, when Satoshi Nakamoto launched the first cryptocurrency blockchain, thousands of cryptocurrencies and different classes of other digital assets have emerged. This section provides a non-exhaustive survey of various cryptocurrencies and some representative features.

Cryptocurrencies

The term *cryptocurrency* generally refers to blockchain-based digital currencies maintained on decentralized networks. For the purposes of this report, *cryptocurrencies* refers to a type of digital asset. Stablecoins (see "Stablecoins" below) are a subset of cryptocurrency. Non-fungible tokens and digital (or metaverse) real estate are other types of digital assets. They use similar technology but are beyond the scope of this report. Other terms used synonymously with cryptocurrency are *crypto asset* and *tokens*, among others. The term *cryptocurrencies* and citation of broad market capitalization often include stablecoins (see "Stablecoins"), which have their own distinct set of properties—most notably that they try to maintain a peg to some underlying asset.

The two most prevalent cryptocurrencies are Bitcoin and Ether, which combined represent around 61% of the entire crypto market.[27] The cryptocurrency market, which consists of between 13,000 and 20,000 cryptocurrencies, according to industry tracking websites, has been characterized by near constant and rapid price increases and price decreases.[28] Most recently, after experiencing exponential growth from 2020 to a record high of nearly $3 trillion in November 2021, the market capitalization fell to less than $800 billion in November 2022. Bitcoin fell from nearly

[24] Garratt, Lee, and Malone, "Token- or Account-Based?"

[25] Yaga et al., *Blockchain Technology Overview*, p. 9.

[26] Yaga et al., *Blockchain Technology Overview*, pp. 9-10.

[27] According to Coinmarketcap.com, as of February 15, 2023, Bitcoin (41.9%) and Ether (18.4%) account for about 60.3% of the market capitalization of all crypto.

[28] See Coingecko.com and Coinmarketcap.com for these figures.

$69,000 to a two-year low of below $16,000 during this time.[29] This trend has been referred to as crypto winter. A host of cryptocurrency project and company failures in summer and fall 2022, including the collapse of FTX, perhaps the most notable to date, were caused—and exacerbated—by this broader market downturn.[30] As of the time of this report, the total crypto market capitalization is around $1 trillion.[31]

Bitcoin

Bitcoin was the first cryptocurrency to gain widespread adoption. Bitcoin runs on a public blockchain, secured by cryptography, and uses the *proof of work* consensus mechanism described above to validate transactions. It also exhibits unique characteristics. For example, the mining and hashing and use of Bitcoin block rewards creates a relationship intended to keep block mining (approval) times roughly stable.[32] The hashing complexity is intended to ensure block approval rates of 10 minutes.[33] If the number of miners or the computing capacity being used increases—perhaps because the Bitcoin block reward induces more miners to compete or deploy more advanced equipment—thus mining blocks faster than 10 minutes (on average), the proof difficulty increases. Alternatively, if the network and its participants mine blocks at a slower rate (perhaps because the number of miners falls), the proof of work difficulty falls, ensuring that the number of active miners is capable of meeting the 10-minute goal.[34] The effort required of the proof of work favors miners with greater computational power requiring significant amounts of energy.[35]

Other notable and interrelated Bitcoin features include transactions fees, a hard cap on the number of Bitcoin, and block reward *halving*. The limit on block approval rates means that transactions are slow compared to traditional payment systems.[36] Network participants can pay *transaction fees* to incentivize miners to process their transactions more quickly. Although the block reward (which is hard-coded into the design) is still the primary form of compensation, transaction fees are expected to grow as block rewards shrink.[37] For approximately every 210,000 blocks, the system "halves" the block reward miners receive for validating transactions. Halving

[29] For Bitcoin prices, see https://fred.stlouisfed.org/series/CBBTCUSD.

[30] See for example, CRS Insight IN11928, *Algorithmic Stablecoins and the TerraUSD Crash*, by Paul Tierno, Andrew P. Scott, and Eva Su; Yueqi Yang and Hannah Miller, "Crypto's Brutal Week Ends with a Trading Halt and Bailout," *Bloomberg*, July 1, 2022, https://www.bloomberg.com/news/articles/2022-07-01/crypto-broker-voyager-digital-suspends-trading-withdrawals; and CRS Insight IN12047, *What Happened at FTX and What Does It Mean for Crypto?*, by Paul Tierno.

[31] See Coinmarketcap.com as of February 15, 2023.

[32] Nakamoto, "Bitcoin: A Peer-to-Peer Electronic Cash System," p. 3; and Andreas M. Antonopoulos, "Mining and Consensus," in *Mastering Bitcoin*, https://www.oreilly.com/library/view/mastering-Bitcoin/9781491902639/ch08.html (O'Reilly).

[33] Antonopoulos, "Mining and Consensus."

[34] Alyssa Hertig, "Bitcoin Halving Explained," *CoinDesk*, March 9, 2022, https://www.coindesk.com/learn/2020/03/24/Bitcoin-halving-explained/.

[35] Joshua A. Kroll, Ian C. Davey, and Edward W. Felten, "The Economics of Bitcoin Mining, or Bitcoin in the Presence of Adversaries," *Twelfth Workshop on the Economics of Information Security (WEIS 2013)*, June 11, 2016, p. 5.

[36] Frederic Boissay et al., "Blockchain Scalability and the Fragmentation of Crypto," *BIS Bulletin*, no. 56 (June 7, 2022), p. 3, https://www.bis.org/publ/bisbull56.pdf.

[37] Miles Carlsten et al., "On the Instability of Bitcoin Without the Block Reward," *Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security*, October 24, 2016, p. 1, https://dl.acm.org/doi/10.1145/2976749.2978408. The concept of fees is also referenced in Nakamoto, "Bitcoin: A Peer-to-Peer Electronic Cash System," p. 3.

occurs roughly every four years.[38] The original block reward was 50 Bitcoin. As of 2022, after three halvings, miners are rewarded 6.25 for each block mined.[39] Finally, the number of Bitcoin created is capped at 21 million, when creation of new Bitcoin is to cease.[40]

Ethereum

Ether is the cryptocurrency native to the Ethereum blockchain, which claims to "build on Bitcoin, with some big differences."[41] In an assessment of Bitcoin, Vitalik Buterin—Ethereum's founder—described Bitcoin as having a "weak version of a concept of 'smart' contracts."[42] Smart contracts are programs or software that can self-execute when various participants meet some predetermined set of criteria. Ethereum thus set out to create an "alternative protocol for building decentralized applications … allowing anyone to write smart contracts and decentralized applications where they can create their own arbitrary rules for ownership, transaction formats and state transition functions."[43] In cryptocurrency and decentralized finance (see "Decentralized Finance (DeFi)" below), smart contracts are often used to facilitate trades between users without an intermediary. Ethereum shares some similarities with Bitcoin, including pseudonymity, immutability, decentralization, and broadly speaking its basic functions as a unit of account and medium of exchange, among others. However, there are some important differences.

Because of the enhanced programmability offered, the Ethereum network has become a favorite foundation for cryptocurrency projects that require a certain level of flexibility afforded by smart contracts, including the creation of additional tokens and the implementation of broader decentralized finance, or *DeFi*, projects.[44]

Bitcoin has only ever been mineable—developed from nothing and with no initial allotment or pre-sale of coins to participants—and has a hard cap of 21 million Bitcoin. This is not the case with Ether. Ether pre-sold a majority of the initially created cryptocurrency (83.5% at the time) in a pre-mine in 2014 and set aside the remainder for accrued expenses and a post-sale reserve.[45] As Ether became mineable and network mining activities created more Ether, the share of pre-mined crypto (those that were purchased prior to the network going live) fell as a percentage of the total outstanding.

While there is no hard cap on the amount of Ether that may ever enter the system, the network recently implemented various upgrades that sought to both limit the creation of new Ether and

[38] Antonopoulos, "Mining and Consensus."

[39] See https://github.com/Bitcoin/Bitcoin/blob/0d20c42a014ff95aab1447a92605c3a194cfeecc/src/validation.cpp#L1080-L1091. At the onset, miners received 50 Bitcoin per block. This was halved to 25 in 2012, to 12.5 in 2016, and to 6.25 in 2020.

[40] Antonopoulos, "Mining and Consensus."

[41] Ethereum, "What Is Ethereum?," https://ethereum.org/en/what-is-ethereum/.

[42] Vitalik Buterin, "A Next-Generation Smart Contract and Decentralized Application Platform," Ethereum, 2014, https://ethereum.org/en/whitepaper/.

[43] Buterin, "A Next-Generation Smart Contract and Decentralized Application Platform."

[44] Ethereum allows user to create additional tokens to run on the Ethereum network using the Ethereum Request for Comment 20 (or ERC-20 standard) and the broader implementation of broader DeFi projects (described in more detail below in "Decentralized Finance (DeFi)"). For example, ERC-20 is a smart contract consisting of a set of standards that developers can use to create tokens that operate on the Ethereum network. For more on ERC-20 tokens, see https://ethereum.org/en/developers/docs/standards/tokens/erc-20/. For more on decentralized finance, see CRS Insight IN11709, *Decentralized Finance (DeFi) and Financial Services Disintermediation: Policy Challenges*, by Eva Su.

[45] Buterin, "A Next-Generation Smart Contract and Decentralized Application Platform."

reduce existing supply.[46] The first of the two changes implemented in the "London upgrade" affected Ether supply. As a result of this upgrade, the network *burns*—or removes from circulation—a certain amount of Ether from the supply with each transaction.[47] In addition, the recent and more momentous upgrade, called "the Merge," drastically reduced the network block reward.[48] Therefore, new Ether supply increases at a much slower pace than before the Merge.[49]

The Merge was arguably one of the biggest things to happen to the Ethereum network since its inception. The Merge shifted the network from *proof of work* to a *proof of stake* consensus protocol.[50] Ethereum, like Bitcoin, was initiated using proof of work but with the ambition from its origins of shifting consensus protocols.[51] Proof of stake is an alternative method for securing a blockchain that proponents believe is less energy intensive.[52] Proof of work requires miners to compete with each other to solve computationally intensive, cryptographically secured puzzles, which prioritize network nodes with computation power. In proof of stake, by contrast, any validating node that "stakes," or deposits, at least 32 Ether enters a pool of potential validators that may be randomly selected to submit the next block.[53] The network can seize validator-staked Ether for malicious activity or other offenses. Ethereum's founder claimed that the shift would reduce the Ethereum network's power consumption and emissions by greater than 99% and reduce global energy consumption by 0.2%.[54]

Stablecoins[55]

Cryptocurrencies such as Bitcoin and Ether fluctuate in value based on market supply and demand. By contrast, stablecoins are digital assets "designed to maintain a stable value relative to a national currency or other reference assets."[56] For example, the Tether stablecoin is tied to the

[46] Taylor Locke, "Ethereum Has Destroyed Almost $6 Billion Worth of Its Own Cryptocurrency on Purpose. Here's Why," *Fortune*, March 2022, https://fortune.com/2022/03/21/ethereum-destroyed-billions-in-ether-supply/. The proposal is the Ethereum Improvement Proposal 1559, or 'London.'

[47] Ethereum, "EIP-1559: Fee Market Change for ETH 1.0 Chain," press release, April 13, 2019, https://eips.ethereum.org/EIPS/eip-1559#eth-burn-precludes-fixed-supply.

[48] What occurred is more technical: Block rewards were swapped for stake or validator rewards, which were capped at about 1,600 per day. Base fees continued to be burned while validators/stakers received priority fees.

[49] Calculated as the number of newly issued ETH/existing supply.

[50] Buterin, "A Next-Generation Smart Contract and Decentralized Application Platform."

[51] Ethereum, "Launching the Ether Sale," press release, July 22, 2014, https://blog.ethereum.org/2014/07/22/launching-the-ether-sale.

[52] For more on the energy requirements and implication of cryptocurrency, see CRS In Focus IF12286, *Recent Cryptocurrency Developments: Energy and Environmental Implications*, by Kristen E. Busch and Corrie E. Clark.

[53] Ethereum, "Proof of Stake (POS)," https://ethereum.org/en/developers/docs/consensus-mechanisms/pos/.

[54] Aoyon Ashraf, "Vitalik Buterin Says Ethereum Merge Cut Global Energy Usage by 0.2%, One of Biggest Decarbonization Events Ever," *CoinDesk*, September 15, 2022, https://www.coindesk.com/business/2022/09/15/vitalik-buterin-says-ethereum-merge-cut-global-energy-usage-by-02-one-of-biggest-decarbonization-events-ever/, and Vitalik Buterin (@VitalikButerin), "'The merge will reduce worldwide electricity consumption by 0.2%' - @drakefjustin," https://twitter.com/VitalikButerin/status/1570299062800510976.

[55] The uses, regulatory treatments, and policy implications of stablecoins are as varied as those of crypto generally, but they are outside the remit of this report. For more on stablecoins, see CRS Insight IN11713, *How Stable Are Stablecoins?*, by Eva Su; CRS In Focus IF11968, *Stablecoins: Background and Policy Issues*, by Eva Su; CRS Legal Sidebar LSB10753, *Stablecoins: Legal Issues and Regulatory Options (Part 1)*, by Jay B. Sykes; and CRS Legal Sidebar LSB10754, *Stablecoins: Legal Issues and Regulatory Options (Part 2)*, by Jay B. Sykes.

[56] President's Working Group on Financial Markets, Federal Deposit Insurance Corporation, and Office of the Comptroller of the Currency, *Report on Stablecoins*, November 1, 2021, https://home.treasury.gov/system/files/136/StableCoinReport_Nov1_508.pdf.

U.S. dollar and set equal in value to $1.[57] Total market capitalization for stablecoins is more than $140 billion.[58] One primary use of stablecoins is trading of other cryptocurrencies. According to an industry data source, nearly 75% of trading on all crypto platforms is between stablecoins and other tokens.[59]

Proponents often point to stablecoins' relative stability as an advantage for their use in payments. However, despite their name, stablecoins do not always maintain their stable value. While stablecoins typically attempt to maintain a peg to a fiat currency, issuers may attempt to achieve this goal in different ways. Certain stablecoins attempt to achieve this peg by holding "reserve assets."[60] Others may use algorithms or smart contracts to manage the supply of tokens and guide their value to various reference assets.[61]

Central Bank Digital Currency[62]

In recent years, the Federal Reserve as well as central banks around the world have begun discussing and exploring the prospect of a central bank digital currency (CBDC). A CBDC can entail many definitions or features. Depending on how they are designed, CBDCs may or may not use similar technologies to existing cryptocurrencies. Broadly, the idea behind CBDCs is that issuing and managing a digital currency by a central bank may realize at least some of the anticipated benefits of cryptocurrencies but with greater efficiency and fewer risks.[63] For example, CBDCs could be used for payments, much the way crypto was originally intended. However, CBDCs would be legal tender and would exist as dollars themselves instead of having values designed to be linked to dollars. Some experts are skeptical of the utility or value of CBDCs given that central-bank-issued currency already is easily and inexpensively exchanged electronically.[64]

In a January 2022 report, the Federal Reserve defined *CBDC* as "as a digital liability of the Federal Reserve that is widely available to the general public."[65] Various central banks and the Bank for International Settlements defined a "general purpose" or retail CBDC as "a digital

[57] Tether stablecoins are also known as USDT; see https://coinmarketcap.com/currencies/tether/. With a market capitalization of more than $68 billion, USDT is the third-largest cryptocurrency.

[58] Coingecko, "Stablecoins by Market Capitalization," https://www.coingecko.com/en/categories/stablecoins.

[59] U.S. Securities and Exchange Commission, "President's Working Group Report on Stablecoins," Chair Gary Gensler comment on Report, November 2021, https://www.sec.gov/news/statement/gensler-statement-presidents-working-group-report-stablecoins-110121#_ftn3. See https://www.theblock.co/data/crypto-markets/spot for recent data.

[60] *Report on Stablecoins*, p. 4.

[61] For more on this form of *algorithmic stablecoins*, see CRS Insight IN11928, *Algorithmic Stablecoins and the TerraUSD Crash*, by Paul Tierno, Andrew P. Scott, and Eva Su.

[62] The policy considerations raised by CBDCs, including their goals and uses, legal requirements, and features and design, are outside the scope of this report. For more information on CBDCs, see CRS Report R46850, *Central Bank Digital Currencies: Policy Issues*, by Marc Labonte and Rebecca M. Nelson.

[63] Kristalina Georgieva, "The Future of Money: Gearing up for Central Bank Digital Currency," speech at the Atlantic Council, February 9, 2022, https://www.imf.org/en/News/Articles/2022/02/09/sp020922-the-future-of-money-gearing-up-for-central-bank-digital-currency.

[64] Sulabh Agarwal and Ousmène Jacques Mandeng, "Why CBDC Stands to Benefit Not Harm Banks," *Accenture Blog*, September 23, 2022, https://bankingblog.accenture.com/why-cbdc-stands-to-benefit-not-harm-banks.

[65] Board of Governors of the Federal Reserve System, *Money and Payments: The U.S. Dollar in the Age of Digital*, January 2022, https://www.federalreserve.gov/publications/files/money-and-payments-20220120.pdf.

payment instrument, denominated in the national unit of account, that is a direct liability of the central bank."[66] Different countries' CBDCs may vary substantially in design and features.[67]

The Biden Administration entered the debate on a U.S. CBDC, noting that one "may have the potential to support efficient and low-cost transactions, particularly for cross-border funds transfers and payments, and to foster greater access to the financial system, with fewer of the risks posed by private sector-administered digital assets."[68] For this reason, the Administration mandated that the Department of the Treasury and various other agencies produce a report on the future of money and include a section on the implications of a CBDC, including for growth and stability.[69] The subsequent report, published in September 2022, was noncommittal and recommended advancing work on a possible CBDC "in case one is determined to be in the national interest."[70] Treasury announced in the report that it will lead an interagency working group to coordinate and consider implications of adopting a CBDC.[71] The working group—which is to consist of the Federal Reserve, the National Economic Council, the National Security Council, the Office of Science and Technology Policy, and the Department of the Treasury—does not appear to have been formed yet.

Ways to Interact with Crypto

The discussion of crypto presented above (see "What Is Cryptocurrency?") provides a description of one type of crypto interactions, called *on-chain* transactions, where users access a decentralized ledger directly. Users may also engage with crypto in intermediated transactions on centralized platforms such as cryptocurrency exchanges and payment companies, called *off-chain* transactions, which is how the vast majority of nonexpert consumers transact in crypto.

On-Chain Transactions

On-chain transactions are transactions processed over the blockchain, the network of nodes that maintain the system publishing ledgers and validating or mining transactions. Users send and receive cryptocurrency on-chain using public and private "keys," which are unique strings of alphanumeric characters.[72]

- *Private keys:* Private keys are codes that secure ownership of cryptocurrency and allow owners to transact with their crypto. Individuals sign transactions in cryptocurrency with private keys. The keys represent ownership, leading some in the industry to coin the expression "not your keys, not your crypto." However, private keys can be long and easily misplaced, leading to other issues.[73]

---

[66] Bank for International Settlements, *Central Bank Digital Currencies: Foundational Principles and Core Features*, October 9, 2020, https://www.bis.org/publ/othp33.htm. The list of central banks includes the Bank of Canada, the European Central Bank, the Bank of Japan, Sveriges Riksbank, Swiss National Bank, the Bank of England, the Federal Reserve, and the Bank for International Settlements.

[67] See CRS Report R46850, *Central Bank Digital Currencies: Policy Issues*, by Marc Labonte and Rebecca M. Nelson.

[68] E.O. 14067, "Executive Order on Ensuring Responsible Development of Digital Assets."

[69] E.O. 14067, "Executive Order on Ensuring Responsible Development of Digital Assets."

[70] U.S. Department of the Treasury, *The Future of Money and Payments: Report Pursuant to Section 4(b) of Executive Order 14067*, September 2022, https://home.treasury.gov/system/files/136/Future-of-Money-and-Payments.pdf.

[71] U.S. Department of the Treasury, *The Future of Money and Payments*.

[72] Public keys are often equated to blockchain addresses. In reality, the addresses are derivations of the public key. See Yaga et al., *Blockchain Technology Overview*, p. 12.

[73] Nathanial Popper, "Lost Passwords Lock Millionaires out of Their Bitcoin Fortunes," *New York Times*, January 12,

- *Public keys and crypto addresses:* Public keys and their related addresses are considered *pseudonymous*, which means that users are identified by their public keys or their derived addresses—not by names, Social Security numbers, or other official forms of identification. Therefore, while the blockchain is public and all transactions are visible, determining the identity behind a public key address is difficult, and tracing transactions requires considerable effort.[74]

For the most part, only cryptocurrencies that are "native" to a blockchain or network are compatible at a network address. For instance, Ether cannot transact on the Bitcoin blockchain, while Bitcoin cannot transact on Ethereum.[75]

Validation and mining, performed by other nodes or users and governed by specific procedures, finalize transactions after users have entered their public and private keys, as described above in the "Blockchain, Decentralized Consensus, and Cryptography" section. Transactions generally require that an initiator remits a fee. Similar to crypto generated from mining, fees compensate miners for their role in maintaining the system. Fees can fluctuate depending on the amount of transactions or congestion on the network at any giving time. The size of a fee offered can influence the processing time.[76]

Users may store and access their cryptocurrency in "wallets"—software or hardware designed to enable transfers of cryptocurrency. Wallets can broadly be grouped into one of three types: custodial, non-custodial, and cold storage. Custodial wallets are provided by centralized intermediaries (which would be said to be acting as "custodians" in traditional finance, hence the moniker) and utilized in off-chain transactions. They are described in more detail in the later section, "Off-Chain Transactions." The remaining two types are used for on-chain transactions:

- **Non-custodial wallets.** Non-custodial wallets are not hosted by third-party institutions but rather managed directly by users to facilitate on-chain transactions. They are pieces of computer software that maintain the public and private key pairs necessary to access and sign the assets for transmission to blockchains and "store the address on a blockchain where a particular asset resides."[77] Non-custodial wallet holders who lose private keys will lose access to the cryptocurrency stored in the wallets.[78] There are no customer identification or know-your-customer checks associated with most of these wallets. Because non-

2021, https://www.nytimes.com/2021/01/12/technology/Bitcoin-passwords-wallets-fortunes.html.

[74] For one academic paper analyzing on-chain activity on the Bitcoin network, see Igor Makarov and Antoinette Schoar, *Blockchain Analysis of Bitcoin Market*, National Bureau of Economic Research (NBER), Working Paper no. 29396, October 2021, https://www.nber.org/papers/w29396. For websites publishing blocks with block details, see, for Bitcoin blockchain, https://blockstream.info/, and for Ethereum network transactions, https://etherscan.io/.

[75] This point is strictly true. However, there are some caveats. The Ethereum network's ERC-20 is a series of standards that allow users to build new tokens on the Ethereum network and underlying technology. Moreover, cryptocurrencies from one blockchain can be "wrapped" (entered into and held in a smart contract) with an equal value offered in exchange on a different blockchain. See Robert Stevens, "What Are Wrapped Tokens?," *CoinDesk*, February 4, 2022, https://www.coindesk.com/learn/what-are-wrapped-tokens/.

[76] Alyssa Hertig, "A Guide to Saving on Bitcoin's High Transaction Fees," *CoinDesk*, February 26, 2021, https://www.coindesk.com/tech/2021/02/26/a-guide-to-saving-on-Bitcoins-high-transaction-fees/.

[77] Lucas Mearian, "What's a Crypto Wallet (and How Does It Manage Digital Currency)?" *Computer World*, April 17, 2019, https://www.computerworld.com/article/3389678/whats-a-crypto-wallet-and-does-it-manage-digital-currency.html.

[78] Alexandra D. Comolli and Michele R. Korver, "Surfing the First Wave of Cryptocurrency Money," *Department of Justice Journal of Federal Law and Practice: Technology and Law*, vol. 69, no. 3 (May 2021), p. 198, https://www.justice.gov/usao/page/file/1403671/download.

custodial wallets do not involve third parties, they do not support purchase or sales of cryptocurrency using fiat currency. That service is provided only by third-party intermediaries. Instead, non-custodial wallet holders can transact only on-chain. Non-custodial wallets are typically formatted to specific blockchains. Holding multiple cryptocurrencies on-chain would require maintaining multiple wallets, although there are some wallets that support multiple coins.

- **Cold-storage wallets.** Cold-storage wallets are pieces of hardware that allow end users to store cryptocurrencies offline, a practice that shields them from hacking. These devices can look and function like USB drives. Users may connect cold-storage wallets to the internet to perform transactions.[79]

Decentralized Finance (DeFi)

On-chain use of cryptocurrency underpins DeFi. *DeFi* generally refers to a use of cryptocurrency and its enabling protocols and technologies (such as digital ledger technology and smart contracts) to operate an alternative financial system that disintermediates traditional financial players such as banks and brokers.[80] While regulated third-party intermediaries such as banks, brokers, and exchanges facilitate transactions in the traditional financial system, DeFi uses various smart contracts to allow any network participant that meets smart contract criteria to directly fill the roles of automated market makers and liquidity providers, among others, to facilitate transactions in crypotocurrency.[81]

Off-Chain Transactions

Off-chain transactions, the far more common form of transaction for consumers without sophisticated expertise, are any transactions that occur outside of, and do not generate transactions on, the main blockchain. Instead, they are generally processed and recorded by intermediaries where customers hold accounts.[82] There are a variety of ways off-chain transactions can occur. Distinct commercial solutions, such as exchanges or payment platforms, operate separately and parallel to blockchain networks to facilitate buying, holding, selling, and trading cryptocurrencies. They hold the cryptocurrencies in custody for users, and transactions occur on private ledgers—essentially the same way they do with banks. Transactions that occur on off-chain platforms usually occur between parties on the same platform and entail physical debiting and crediting of digital balances. Unlike on-chain transactions, these platforms are intermediated, are typically instantaneous, may have lower fees, and allow participants to hold multiple cryptocurrencies in their wallets or accounts.[83]

---

[79] See footnote 32 in Comolli and Korver, "Surfing the First Wave of Cryptocurrency Money," p. 198. See also Jake Frankenfield, "Cold Storage: What It Is, How It Works, Theft Protection," *Investopedia*, October 4, 2022, https://www.investopedia.com/terms/c/cold-storage.asp.

[80] U.S. Department of the Treasury, *Crypto-Assets: Implications for Consumers, Investors, and Businesses*, September 2022, p. 10, https://home.treasury.gov/system/files/136/CryptoAsset_EO5.pdf.

[81] *Automated market makers* (AMMs) use smart contracts to define the prices of assets. AMMs often use equations to balance the supply of trading pairs. *Liquidity providers* provide liquidity to AMMs to balance the supply of trading pairs in exchange for fees and governance tokens. For definitions, see Andrey Sergeenkov, "What Is an Automated Market Maker?," *CoinDesk*, March 9, 2022, https://www.coindesk.com/learn/2021/08/20/what-is-an-automated-market-maker/. For more on DeFi, see CRS Insight IN11709, *Decentralized Finance (DeFi) and Financial Services Disintermediation: Policy Challenges*, by Eva Su.

[82] Xenia Soares, "On-Chain vs. Off-Chain Transactions: What's the Difference?" *CoinDesk*, https://www.coindesk.com/learn/on-chain-vs-off-chain-transactions-whats-the-difference/.

[83] Soares, "On-Chain vs. Off-Chain Transactions."

- **Custodial wallets.** Custodial wallets, also referred to as *hosted wallets*, are maintained by third-party institutions that facilitate off-chain transactions, including crypto exchanges and payment applications with crypto offerings. Because a third party maintains a custodial wallet, loss of a security key or password does not result in loss of the wallet's contents. Like conventional digital wallets, customers may fund custodial crypto wallets using bank accounts, but they can also accept transfers from non-custodial wallets. While most custodial crypto wallets offer the option to buy, sell, or trade certain digital assets, only some allow payments and transfers. Digital asset platforms execute transactions for third-party custodial wallets on the account holder's behalf and record them on the books of the custodian (or "off-chain") rather than on the distributed ledger blockchain of the coin.

Cryptocurrency Exchanges

Cryptocurrency exchanges are online platforms where users can buy, sell, and trade various cryptocurrencies. The digital assets are stored in a custodial wallet, which is essentially an account that shares more in common with a typical investment account than a non-custodial wallet. While centralized exchanges may provide a more "user-friendly" interface with crypto, they do so by replacing many of the unique aspects of crypto with an entity that resembles a traditional financial institution but without the same regulation. Unlike the process in on-chain transactions, interacting with cryptocurrency through exchanges is centralized, and individuals must often use government identification or Social Security numbers and provide addresses to transact. They may also hold multiple coins—offerings vary by exchange—in their wallets. Failures among centralized crypto institutions have created an internecine feud between proponents of decentralization and others that support intermediaries.

Typically, exchanges do not execute customer transactions directly on the blockchain of the specific currency traded. The transactions do not require the exchange of public and private keys, nor are the other actions associated with on-chain transactions, such as mining, conducted. Instead, exchanges "match client transactions on an internalized offchain basis, in over the counter markets, or by using the company's own assets."[84] Exchanges typically record customer transactions on the blockchain of a specific cryptocurrency only when a user withdraws the currency from the exchange to an address on the blockchain (in other words, from a hosted wallet to an unhosted wallet). Crypto exchanges are described as offering "borderless" assets but operate like closed loops with internal supply and demand dynamics that can often lead to different prices for the same assets across platforms.[85] Such price discrepancies may lead arbitrage traders to exploit these differences for financial gain.[86]

[84] Izabella Kaminska, "Why Coinbase's Stellar Earnings Are Not What They Seem," *Financial Times*, April 8, 2021, https://www.ft.com/content/cadd6eba-1dd7-4f31-94e0-2dc43ace7b0f. This article explains the mechanics of Coinbase, which are assumed to be roughly similar across other exchanges.

[85] Bob Pisani and Todd Haselton, "Here's Why Bitcoin Prices Are Different on Each Exchange," *CNBC*, December 12, 2017, https://www.cnbc.com/2017/12/12/why-Bitcoin-prices-are-different-on-each-exchange.html.

[86] Andrewy Sergeenkov, "Crypto Arbitrage Trading: How to Make Low-Risk Gains," *CoinDesk*, March 2022, https://www.coindesk.com/learn/crypto-arbitrage-trading-how-to-make-low-risk-gains/.

Crypto on Payments Apps

Payments platforms such as PayPal, Venmo, and Cash App, among others, also allow customers to buy and hold cryptocurrencies off-chain.[87] The specific cryptocurrencies supported, services permitted, and type of ownership offered differ by platform. PayPal advertises that its users can buy, hold, transfer, and sell four cryptocurrencies: Bitcoin, Bitcoin Cash, Ethereum, and Litecoin. Notably, PayPal's crypto terms of service are clear that individuals do not own a "specific, identifiable, Crypto Asset," that the company combines users' crypto balances in one or more omnibus accounts, and that users own the "right" to the asset as well as the asset's gains or losses.[88] While that distinction is not necessarily problematic, it may be consequential if the platform is offline or its crypto portal is not functioning appropriately when an individual wants to make a transaction. Some platforms allow users to download their crypto to unhosted wallets, while others allow users to maintain it solely on their platforms. PayPal allows users to make purchases with crypto. In such transactions, PayPal facilitates a sale of cryptocurrencies, the fiat currency proceeds from which are used to make purchases.[89]

Traditional Financial Institutions and Crypto

Traditional financial institutions, including banks and asset managers, have also begun participating in the crypto ecosystem. This section highlights some examples of the ways traditional financial institutions are integrating cryptocurrency into their offered services. It is not intended to be an exhaustive review of all existing relationships or potential partnerships in the industry.

Conceptually, banks can participate in crypto markets directly by offering crypto products such as loans backed by crypto collateral or crypto investments. They can also gain indirect exposure to crypto by offering traditional banking services to crypto firms. Alternatively, crypto firms may seek bank charters, and bank holding companies may seek to form crypto subsidiaries, thus providing other channels through which the banking system and crypto can interact.[90]

One way banks participate in crypto is through offering custody services. *Custody services* is generally defined as settlement, safekeeping, and reporting of customers' marketable securities.[91] Some banks offer these types of services in addition to their core banking activities, while others focus specifically on custody and fiduciary activities.[92] Bank of New York Mellon (BNY), for example, the largest custodian bank, provides primary custodial services of reserves for the USD

[87] PayPal, "PayPal Launches New Service Enabling Users to Buy, Hold and Sell Cryptocurrency," press release, October 2020, https://newsroom.paypal-corp.com/2020-10-21-PayPal-Launches-New-Service-Enabling-Users-to-Buy-Hold-and-Sell-Cryptocurrency; PayPal, "Customers Can Now Buy, Hold and Sell Cryptocurrency Directly Within the Venmo App with as Little as $1," press release, April 20, 2021, https://newsroom.paypal-corp.com/2021-04-20-Introducing-Crypto-on-Venmo.

[88] PayPal, "PayPal Cryptocurrency Terms and Conditions," last updated December 14, 2022, https://www.paypal.com/us/webapps/mpp/ua/cryptocurrencies-tnc?locale.x=en_US.

[89] PayPal, "PayPal Cryptocurrency Terms and Conditions."

[90] Federal Reserve System, Federal Deposit Insurance Company, and Office of the Comptroller of the Currency, *Joint Statement on Crypto-Asset Risks to Banking Organizations*, January 2023, https://www.federalreserve.gov/newsevents/pressreleases/files/bcreg20230103a1.pdf.

[91] See Office of the Comptroller of the Currency, "Custody Services," https://www.occ.treas.gov/topics/supervision-and-examination/capital-markets/asset-management/custody-services/index-custody-services.html.

[92] For more on custody services, see CRS In Focus IF11997, *Bank Custody, Trust Banks, and Cryptocurrency*, by Andrew P. Scott.

Coin (USDC), a stablecoin issued by Circle.[93] In addition, BNY announced in October 2022 that it would permit select clients to hold and transfer Bitcoin and Ether.[94] State Street Bank is also reportedly considering offering this service.[95]

Silvergate, a regional bank member of the Federal Reserve System, offers more specialized crypto-related services, including the Silvergate Exchange Network (SEN). SEN is a network that allows its various crypto clients to send U.S. dollars and euros among themselves, "enabling near real-time transfers and immediate availability of funds."[96] The bank also advertised Bitcoin-collateralized lending.[97]

Asset managers have also begun engaging in crypto activity. For example, Fidelity recently began allowing their employees to invest a portion of their retirement accounts in Bitcoin.[98] BlackRock announced in August 2022 that it launched a spot Bitcoin private trust, which it offers to institutional investors.[99]

Selected Policy Issues

The relative novelty of how cryptocurrency transactions occur—especially in contrast to traditional finance—introduces a host of policy issues. Moreover, recent events, including concern over the potential use of crypto to evade sanctions on Russia and the failure of various cryptocurrency platforms, have increased the attention these policy issues have drawn. This section assesses policy issues that may be of interest to Congress, including, among others, the need to balance competing priorities of privacy and security and the evolving state of regulation.

Inclusion and Scalability

Crypto industry proponents often cite a purported potential to improve financial inclusion as a rationale for crypto.[100] In its current form, the technology does not live up to this promise of

[93] Circle Internet Financial, "Circle Selects BNY Mellon to Custody USDC Reserves," press release, March 31, 2022, https://www.prnewswire.com/news-releases/circle-selects-bny-mellon-to-custody-usdc-reserves-301514681.html.

[94] BNY Mellon, "BNY Mellon Launches New Digital Asset Custody Platform," press release, October 11, 2022, https://www.bnymellon.com/us/en/about-us/newsroom/press-release/bny-mellon-launches-new-digital-asset-custody-platform-130305.html.

[95] Yueqi Yang, "Wall Street Courts Crypto Custody, but with Fingers Crossed," October 27, 2022, https://www.bloomberg.com/news/newsletters/2022-10-27/bny-mellon-bk-state-street-stt-court-crypto-custody-with-fingers-crossed.

[96] See Silvergate Bank, "Silvergate Exchange Network," https://www.silvergate.com/solutions/digital-currency/sen.

[97] See Silvergate Bank, "SEN Leverage," https://www.silvergate.com/solutions/digital-currency/sen-leverage.html.

[98] Fidelity, "A First-of-Its-Kind Investment Account Opportunity," press release, https://www.fidelityworkplace.com/s/digitalassets.

[99] Scott Chipolina and Brooke Masters, "BlackRock Pushes into Crypto Market with Bitcoin Private Trust," *Financial Times*, August 11, 2022, https://www.ft.com/content/0948f1a9-ad0b-4126-9ae8-5ce4e212c07e.

[100] See for example Christine Moy and Jill Carlson, *Cryptocurrencies Can Enable Financial Inclusion. Will You Participate?*, World Economic Forum, June 9, 2021, https://www.weforum.org/agenda/2021/06/cryptocurrencies-financial-inclusion-help-shape-it/; and Jack Dorsey and Alex Gladstein, "Bitcoin 2021: Banking the Unbanked," June 5, 2021, https://www.youtube.com/watch?v=rSSnyJpFNZU. Also, see U.S. House Committee on Financial Services, "Waters Delivers Opening Statement at Full Committee Hearing On the President's Working Group Report on Stablecoins," press release, February 8, 2022, https://financialservices.house.gov/news/documentsingle.aspx?DocumentID=409075. Rep. Waters in her opening statement addresses the need to ensure "financial inclusion is front and center." See also Ritchie Torres, "A Liberal Case for Cryptocurrency," *The Daily News*, May 17, 2022, https://www.nydailynews.com/opinion/ny-oped-a-liberal-case-for-cryptocurrency-20220317-

inclusion, as adoption rates remain low due in part to scalability issues (i.e., the ability to work efficiently as a payment tool at large volumes). Some believe it may be harmful. According to a report produced in response to Executive Order 14067:

> While the data for populations vulnerable to disparate impacts remains limited, available evidence suggests that crypto-asset products may present heightened risks to these groups, and the potential financial inclusion benefits of crypto-assets largely have yet to materialize.[101]

The pro-inclusion argument focuses on certain aspects of crypto, including its availability to anyone with an internet connection, its accessibility or storage anywhere, and dispensation with the need for trust.[102] Regardless of the merits of these arguments, however, cryptocurrency has not caught on as a payment tool. Moreover, use of crypto, especially for payments, is generally considered to be less efficient—it is costlier and slower to settle—than traditional methods of payments.[103] According to researchers at the Bank for International Settlements, "inherent limitations of blockchains," including the incentive structure and the fragmentation of disparate decentralized networks, prevent any one cryptocurrency blockchain from scaling, or growing to accommodate more users efficiently.[104] As such, whereas Visa can reportedly process between 1,700 and 24,000 transactions per second, it takes 10 minutes to process a block containing a transaction on the Bitcoin blockchain, resulting in an average of three to four transactions processed each second.[105] (Ethereum times are slightly better.[106]) Fees for crypto transactions can also be significant, especially when the networks are busy processing many transactions, whereas fees on traditional networks are between 1% and 3% of a transaction.[107]

Beyond the limitations and costs of its payment application, critics question crypto's potential as a "wealth-building tool."[108] Citing crypto's failure to develop "past the use case as a speculative

---

n6iaevmh5jeszkpiaqwcog742q-story.html.

[101] U.S. Department of the Treasury, *Crypto-Assets: Implications for Consumers, Investors, and Businesses*, September 2022.

[102] Trust is cited as a primary reason some individuals refuse to participate in the traditional banking system. See, for example, Paola Boel and Peter Zimmerman, "Unbanked in America: A Review of the Literature," *Economic Commentary*, vol. 2022, no. 7 (May 2022), https://www.clevelandfed.org/en/newsroom-and-events/publications/economic-commentary/2022-economic-commentaries/ec-202207-unbanked-in-america-a-review-of-the-literature.aspx.

[103] Paul Vigna, "Why Bitcoin Hasn't Gained Traction as a Form of Payment," *Wall Street Journal*, February 9, 2021, https://www.wsj.com/articles/why-Bitcoin-hasnt-gained-traction-as-a-form-of-payment-11612886974. While Bitcoin settlement is faster than traditional card network settlements that affect merchants, payments are instantaneous for payers/customers.

[104] Boissay et al., "Blockchain Scalability and the Fragmentation of Crypto."

[105] Visa, "Visa Acceptance for Retailers," https://usa.visa.com/run-your-business/small-business-tools/retail.html. Visa transaction estimates are based on average daily transactions processed divided by seconds in a day. The 24,000 figure was achieved in test conditions. For information on Bitcoin average daily transactions, see Bitcoin, "Frequently Asked Questions," https://Bitcoin.org/en/faq#transactions, and https://ycharts.com/indicators/Bitcoin_transactions_per_day. See also Kyle Croman et al., "On Scaling Decentralized Blockchains (a Position Paper)," *International Conference on Financial Cryptography and Data Security*, August 31, 2016, p. 108, https://doi.org/10.1007/978-3-662-53357-4_8.

[106] Boissay et al., "Blockchain Scalability and the Fragmentation of Crypto," p. 3.

[107] Boissay et al., "Blockchain Scalability and the Fragmentation of Crypto," p. 3. For average Ethereum transaction fees, see BitInfoCharts, "Ethereum Avg. Transaction Fee Historical Chart," https://bitinfocharts.com/comparison/ethereum-transactionfees.html#3y. While fees for both cryptocurrencies are relatively low, average Bitcoin fees were $62 in April 2021. Crypto proponents typically point to Layer 2 solutions such as the Bitcoin Lightning network as ways the industry is providing solutions to scalability. Layer 2 solutions are built "on top of" the public chain, "inherit" the base network's security, and typically aim to expand its scalability and efficiency by moving computation off-chain to enable privacy or save computing resources. Despite these claims, Layer 2 solutions have also been slow to catch on.

[108] Tonantzin Carmona, "Debunking the Narratives About Cryptocurrency and Financial Inclusion," Brookings

asset," one skeptic notes that crypto's ability to "quickly drop to nothing" is particularly risky for populations that structurally have the least financial cushion to fall back on after losses.[109] Similarly, crypto may also exhibit characteristics of "predatory inclusion," wherein access to the innovation with high risks and without appropriate consumer benefits had adverse consequences for participants.[110] Failure and fraud at firms with large retail trades accentuate these drawbacks.

Privacy versus Security

Some individuals are attracted to cryptocurrency because its *pseudonymous* nature may be an advantage in a legitimate desire for privacy from government. However, the same characteristics that provide that privacy may also make crypto a useful tool for engaging in illicit activity. The extent of cryptocurrency's association with money laundering and other forms of illicit activity is the subject of considerable debate. Older research suggested that illicit finance represented nearly half of all Bitcoin activity.[111] A more recent study estimates it to be 3%, while industry analysis places the figure for all of cryptocurrency (not just Bitcoin) as low as 0.15%.[112] Therefore, the practical considerations of balancing the potential privacy provided by cryptocurrency's pseudonymity with the requirement that financial institutions comply with the Bank Secrecy Act (BSA) to implement anti-money laundering (AML) and "know your customer" programs has emerged as a fundamental policy issue.[113]

The balance of privacy and security depends in large part on whether transactions occur off-chain on centralized platforms or via on-chain transactions. Exchanges and other third-party platforms that allow users to hold and transfer crypto must comply with the BSA and implement customer identification programs (see "Applicable Money Services Businesses Framework" below). These programs may limit the ability of bad actors to use exchanges for illicit activities, although some reports have found exchanges' implementation of these programs to be lacking.[114]

Applying AML regulations to on-chain transactions is not as simple. In on-chain transactions, neither participants nor facilitators need to seek approval to submit or validate transactions, respectively. Similarly, transactions do not require approvals from intermediaries that are the hallmark of trust-based traditional financial systems. These transactions contain some impediments to money laundering—they are publicly visible to regulators and blockchain

Institution, October 26, 2022, https://www.brookings.edu/research/debunking-the-narratives-about-cryptocurrency-and-financial-inclusion/.

[109] Carmona, *Debunking the Narratives About Cryptocurrency and Financial Inclusion*.

[110] Carmona, *Debunking the Narratives About Cryptocurrency and Financial Inclusion*.

[111] Sean Foley, Jonathan R. Karlsen, and Talis J. Putnins, "Sex, Drugs, and Bitcoin: How Much Illegal Activity Is Financed Through Cryptocurrencies?," *Review of Financial Studies*, October 21, 2018.

[112] Makarov and Schoar, "Blockchain Analysis of the Bitcoin Market"; and, Chainalysis, "Crypto Crime Trends for 2022: Illicit Transaction Activity Reaches All-Time High in Value, All-Time Low in Share of All Cryptocurrency Activity," press release, January 6, 2022, https://blog.chainalysis.com/reports/2022-crypto-crime-report-introduction/.

[113] 31 U.S.C. §5311 et seq.

[114] Financial Crimes Enforcement Network, *FinCEN Guidance: Application of FinCEN's Regulations to Certain Business Models*, May 9, 2019, https://www.fincen.gov/sites/default/files/2019-05/FinCEN%20Guidance%20CVC%20FINAL%20508.pdf. For a report of lax AML and "know your customer" implementation, see Angus Berwick and Tom Wilson, "How Crypto Giant Binance Became a Hub for Hackers, Fraudsters and Drug Traffickers," Reuters, June 6, 2022, https://www.reuters.com/investigates/special-report/fintech-crypto-binance-dirtymoney/; and, U.S. Department of the Treasury, "OFAC Settles with Virtual Currency Exchange Kraken for $362,158.70 Related to Apparent Violations of the Iranian Transactions and Sanctions Regulations," November 28, 2022, https://home.treasury.gov/system/files/126/20221128_kraken.pdf.

analysts—and funds may be traced using chain analytics and users' public key addresses.[115] Still, various tools—including privacy-enhanced blockchains that obscure addresses and services such as mixers and tumblers—obfuscate analysts and hamper detection.[116] As such, attempts to apply similar regulations to pseudonymous participants, verified by miners and validators that might also sit outside of the sender's jurisdiction, may not be feasible or practical.

Because cryptocurrencies are not a widely accepted form of payment, most users must convert their holdings to fiat currency if they want to buy goods or services, putting a large responsibility on exchanges that do not have long track records with AML compliance.

Existing Regulation of Cryptocurrency

The financial industry is subject to an array of regulations. The goals of various regulations include promoting market integrity and efficiency, consumer and investor protection, and financial stability, among others. Regulations can be prudential (i.e., aimed at creating safety and soundness); require disclosure and reporting; set standards; and create limits on prices and rates.[117] Finally, regulations may be applied to institutions, markets, or activities.[118] One simplified example of this framework is that regulators use disclosure and reporting requirements to regulate the securities industry with the goal of promoting market integrity and efficiency and promoting investor protection. Unlike banks, which have stricter prudential requirements, securities regulation is intended to inform investors about risks and allow them to make their decisions accordingly. Policymakers must balance the costs of regulation (e.g., barriers to entry, cost of capital) with benefits (e.g., efficiency, customer protection).

The regulation of cryptocurrency is unsettled and evolving. Currently, there is not a comprehensive framework for regulating the range of cryptocurrencies, other digital assets, and trading platforms that parallels regulation of securities or commodities. Neither Congress nor federal regulators have created new comprehensive rules specific to crypto. Instead, various state and federal financial industry regulators apply existing regulations to cryptocurrencies and digital asset exchanges using legal categories developed for traditional financial products and services. Those rules have primarily been applied through enforcement on a case-by-case basis rather than through rulemaking, meaning firms may operate in violation of rules for extended periods of time before enforcement actions are undertaken.

Regulators may treat digital assets as securities, commodities, or payment platforms depending on the specific circumstances. For example, cryptocurrency exchanges are licensed at the state level and register with the Financial Crimes Enforcement Network (FinCEN) as money services businesses. Meanwhile, the chairs of both the Commodity Futures Trading Commission (CFTC) and Securities and Exchange Commission (SEC) have issued guidance and enforcement actions and have brought litigation arguing that some digital assets are commodities and others securities

[115] For an example of how chain analysis has been implemented, see U.S. Department of Justice, "Two Arrested for Alleged Conspiracy to Launder $4.5 Billion in Stolen Cryptocurrency," press release, February 8, 2022, https://www.justice.gov/opa/pr/two-arrested-alleged-conspiracy-launder-45-billion-stolen-cryptocurrency.

[116] For a discussion of some of these issues, see CRS Insight IN11920, *Russian Sanctions and Cryptocurrency*, by Kristen E. Busch and Paul Tierno.

[117] For a complete look at financial regulation, see CRS Report R44918, *Who Regulates Whom? An Overview of the U.S. Financial Regulatory Framework*, by Marc Labonte.

[118] CRS Report R44918, *Who Regulates Whom? An Overview of the U.S. Financial Regulatory Framework*, by Marc Labonte.

under their respective jurisdictions, but they have not reached a consensus.[119] Part of the problem is disagreement about what cryptocurrency is from a legal perspective. Regulators have broad authority to interpret traditional rules as applicable to crypto, but those interpretations may be challenged in court with industry-wide implications. As a result, which rules apply to cryptocurrency varies by product, and whether they are applied consistently, are being determined on an ongoing basis. Moreover, regulation is not binary: Crypto firms may be regulated in some activities or aspects and not in others.

This report does not discuss regulation of stablecoins, which face a unique set of policy issues and proposals—although some of the issues discussed below are also relevant to stablecoin regulation. Nor does it focus on how specific types of digital assets are regulated, including, for example, which types of assets SEC has jurisdiction over versus those it does not regulate.

Applicable SEC Framework

Securities most often refers to equity (or stock) and debt (bonds) and "investment contracts," which companies use to fund themselves and their operations.[120] In the more than a decade since the founding of the first cryptocurrency, various observers, including the previous and current chairs of the SEC, have asserted that some cryptocurrencies are securities and should be regulated the same way.[121] (The designation of certain digital assets as securities has emerged as another key policy issue. For a comprehensive look of digital asset securities, see CRS Report R46208, *Digital Assets and SEC Regulation*, by Eva Su.)

In an April 2022 speech, SEC Chair Gary Gensler stated that "many of the tokens trading on these [crypto trading and lending platforms] may well meet the definition of 'securities.'"[122] Notably, Gensler has also said that Bitcoin is likely not a security.[123] The implications for these two views suggests a regulatory environment in which a platform that trades a cryptocurrency the SEC deems to be a commodity may be subject to SEC regulation. But it is unclear whether SEC jurisdiction would apply to non-securities trades on that same platform.

The SEC has also produced a framework it considers when evaluating whether digital assets meet the definition of *investment contract* and should subsequently be subject to securities

[119] For example, CFTC Chair Rostin Benham believes both Bitcoin and Ether are commodities, while SEC Chair Gensler has agreed only that Bitcoin is. Chris Brummer, "DC Fintech Week 2022," https://www.youtube.com/watch?v=Kzcb9cRlEpI&t=11197s (the relevant interview begins at 3 hours, 5 minutes); "Bitcoin, Ethereum Are Commodities, Says CFTC Chair Rostin Behnam," *CNBC*, May 16, 2022, https://www.cnbc.com/video/2022/05/16/bitcoin-ethereum-are-commodities-says-cftc-chair-rostin-behnam.html; and Gary Gensler, "Kennedy and Crypto," SEC, September 8, 2022, https://www.sec.gov/news/speech/gensler-sec-speaks-090822.

[120] The actual definition of *securities* is considerably longer and may be found in Section 2(a)(1) of the Securities Act of 1933, Section 3(a)(10) of the Securities Exchange Act of 1934, Section 2(a)(36) of the Investment Company Act of 1940, and Section 202(a)(18) of the Investment Advisers Act of 1940.

[121] Testimony of SEC Chair Jay Clayton in U.S. Congress, Senate Committee on Banking, Housing, and Urban Affairs, *Chairman's Testimony on Virtual Currencies: The Roles of the SEC and CFTC*, February 6, 2018, https://www.sec.gov/news/testimony/testimony-virtual-currencies-oversight-role-us-securities-and-exchange-commission.

[122] Gary Gensler, "Prepared Remarks of Gary Gensler on Crypto Markets Penn Law Capital Markets Association Annual Conference," SEC, April 4, 2022, https://www.sec.gov/news/speech/gensler-remarks-crypto-markets-040422.

[123] For example, see Benjamin Pimentel, "Gensler: Bitcoin May Be a Commodity," *Protocol*, May 23, 2022, https://www.protocol.com/fintech/gensler-sec-Bitcoin-commodity; and Andrew Ackerman, "SEC's Gensler Signals Support for Commodities Regulator Having Bitcoin Oversight," *Wall Street Journal*, September 8, 2023, https://www.wsj.com/articles/secs-gensler-supports-commodities-regulator-having-Bitcoin-oversight-11662641115.

regulations.[124] Traditionally, the SEC has used the *Howey Test* to determine whether any investment contract—not just cryptocurrencies—is a security. According to the Howey Test, an investment contract is defined by four key features: (1) the investment of money (2) in a common enterprise (3) with a reasonable expectation of profits and (4) to be derived from the efforts of others.[125] The framework provides additional details describing each prong of this test. Notably, whether a particular cryptocurrency qualifies as a "security" under the Howey Test depends on the "specific facts and circumstances" of each asset and whether the various thresholds of the definition are met.[126] The SEC has also brought several enforcement actions against cryptocurrency issuers for failing to register their cryptocurrencies as "securities" or failing to receive exemptions prior to conducting securities offerings.[127]

There is also the issue of implementation. As discussed above, the SEC has been clear it believes that the laws and regulations that apply to traditional securities apply to many cryptocurrencies and exchanges, that this existing regime is adequate to regulate them, and that both should register with the agency.[128] Notably, none of the largest crypto exchanges by volume has registered as a national securities exchange. However, the SEC has not created any new regulations or registration processes tailored for crypto. In March 2022, the SEC proposed amending the definition of *exchange* to include "Communication Protocol Systems," which some believe would "capture" digital asset platforms.[129] To date, no further rulemaking has been undertaken relating to that proposal.[130] While some crypto platforms have registered as alternative trading systems (ATSs), none of the largest crypto exchanges by volume have filed as an ATS, and the SEC chairman has suggested it is an imperfect solution.[131] Similarly, while some cryptocurrencies have registered with the SEC, none with any significant market capitalization has done so.[132] The fact that most cryptocurrencies and platforms have not registered with the

[124] SEC, "Framework for 'Investment Contract' Analysis of Digital Assets," April 3, 2019, https://www.sec.gov/corpfin/framework-investment-contract-analysis-digital-assets.

[125] SEC, "Framework for 'Investment Contract' Analysis of Digital Assets." The Howey Test derives from the Supreme Court's decision in SEC v. W.J. Howey Co., 328 U.S. 293 (1946). See also CRS Report R45301, *Securities Regulation and Initial Coin Offerings: A Legal Primer*, by Jay B. Sykes.

[126] SEC, "Framework for 'Investment Contract' Analysis of Digital Assets."

[127] See, for example, SEC v. Telegram Group Inc., 448 F. Supp. 3d 352 (S.D.N.Y. 2020); SEC v. Kik Interactive Inc., 492 F. Supp. 3d 169 (S.D.N.Y. 2020); SEC Release No. 10445, Order Instituting Cease-and-Desist Proceedings Pursuant to Section 8A of the Securities Act of 1933, Making Findings, and Imposing a Cease-and-Desist Order, In the Matter of Munchee Inc. (December 11, 2017).

[128] SEC, "What Are Crypto Trading Platforms? Office Hours with Gary Gensler," July 28, 2022, https://www.youtube.com/watch?v=aWl55tTZ50Q.

[129] SEC, "Amendments Regarding the Definition of 'Exchange' and Alternative Trading Systems (ATSs) That Trade U.S. Treasury and Agency Securities, National Market System (NMS) Stocks, and Other Securities," 87 *Federal Register*, March 18, 2022.

[130] Gensler, "Prepared Remarks of Gary Gensler on Crypto Markets Penn Law Capital Markets Association Annual Conference."

[131] SEC, "Data: Alternative Trading System ('ATS') List," press release, November 2022, https://www.sec.gov/foia/docs/atslist; and Gensler, "Prepared Remarks of Gary Gensler on Crypto Markets Penn Law Capital Markets Association Annual Conference." Some of the ATSs use blockchain technology to provide market services. According the SEC, "An ATS is a trading system that meets the definition of 'exchange' under federal securities laws but is not required to register as a national securities exchange if the ATS operates under the exemption provided under Exchange Act Rule 3a1-1(a)."

[132] See Christopher Murrer, "U.S. SEC Approves the First Full Securities Registration for a Company Issuing Crypto-Tokens," *A Blog by Baker McKenzie*, August 31, 2020, https://blockchain.bakermckenzie.com/2020/08/31/u-s-sec-approves-the-first-full-securities-registration-for-a-company-issuing-crypto-tokens/; and Daniel Kuhn, "SEC Gives YuNow's Etehereum Token 'Props' RegA+ Approval," *CoinDesk*, July 11, 2019, https://www.coindesk.com/markets/

SEC but continue to operate unimpeded, seemingly counter to the SEC officials' public pronouncements, may create confusion in the marketplace over what is required of various participants under existing laws and regulations.

Applicable CFTC Framework

The CFTC was established in 1974 to regulate commodities futures and options markets originally dominated by agricultural products but extended to include contracts based on financial variables.[133] The CFTC administers the Commodity Exchange Act (CEA), which defines *commodities* as various agricultural products, including wheat, cotton, rice, among others, as well as "all services, rights, and interests … in which contracts for future delivery are presently or in the future dealt in."[134]

In 2014, the CFTC chairman at the time identified the CEA's broad definition of the term *commodity* as the basis for the agency's role in regulating virtual currency derivatives. The chairman noted, "While the CFTC does not have policies and procedures specific to virtual currencies like Bitcoin, the agency's authority extends to futures and swaps contracts in any commodity," which he asserted the CEA defines "very broadly."[135] The CFTC's chair thus said that "[d]erivative contracts based on a virtual currency represent one area within our responsibility."[136]

The CFTC reiterated that interpretation shortly thereafter in a September 2015 enforcement action against a company named Coinflip that operated Derivabit, a Bitcoin options and futures platform. In the enforcement action, the CFTC concluded that Bitcoin and other virtual currencies are "commodities."[137] A separate federal court decision later supported the CFTC's position. In *CFTC v. McDonnell*, a federal district court ruled that the CEA's definition of the term *commodity* encompasses virtual currency.[138]

Currently, the CFTC implements its authority over digital assets through enforcement actions and guidance.[139] CFTC-registered entities allow trading of futures and options for Bitcoin and Ether, which trade on various CFTC-registered designated contract markets and are cleared by registered derivatives clearing organizations.[140]

2019/07/11/sec-gives-younows-ethereum-token-props-reg-a-approval/.

[133] See CRS Report R43117, *The Commodity Futures Trading Commission: Background and Current Issues*, by Rena S. Miller.

[134] 7 U.S.C. §1a(9).

[135] Testimony of CFTC Chairman Timothy Massad, in U.S. Congress, Senate Committee on Agriculture, Nutrition and Forestry, December 10, 2014, https://www.cftc.gov/PressRoom/SpeechesTestimony/opamassad-6.

[136] Testimony of Massad, in U.S. Congress, Senate Committee on Agriculture, Nutrition and Forestry.

[137] CFTC Order Coinflip, Inc. d/b/a Derivabit, et al., Respondents, Dkt. No. 15-29 (CFTC September 17, 2015), http://www.cftc.gov/idc/groups/public/@lrenforcementactions/documents/legalpleading/enfcoinfliprorder09172015.pdf, *United States of America Before the Commodity Futures Trading Commission*, (CFTC Docket No.15-29).

[138] CFTC v. McDonnell, 287 F. Supp. 3d 213, 216 (E.D.N.Y. 2018).

[139] CFTC, "What Is a Bitcoin Futures ETF?," https://www.cftc.gov/LearnAndProtect/AdvisoriesAndArticles/BitcoinFuturesETF.html.

[140] See, for example, CFTC, "CFTC Grants DCO Registration to LedgerX LLC," press release, July 24, 2017, https://www.cftc.gov/PressRoom/PressReleases/7592-17.

The CFTC's authority in spot markets is limited to enforcing prohibitions on fraud and manipulation.[141] Some observers have concluded that a large amount of fraud in these markets escapes enforcement—an outcome that may be attributable to the CFTC's small size and limited resources.

Applicable Bank Framework

At the federal level, there are ostensibly two ways banks can participate in the crypto landscape. First, national banks can seek approval from the Office of the Comptroller of the Currency (OCC) to provide limited crypto services. These services include crypto custody services, holding stablecoin reserves, and using node verification networks and stablecoin for payments.[142] In November 2021, the OCC published Interpretive Letter 1179, confirming three earlier letters that permitted nationals banks to provide the aforementioned services if they can do so "in a safe and sound manner" and only after the banks first notified their supervisory offices and received written approval.[143] Second, an institution may seek a national bank trust charter, which limits the holder to "fiduciary capacity" operations permitted by federal statute and laws in the states where the trust bank or company is located.[144] The OCC has recently approved three limited purpose national bank trust charters for three cryptocurrency native firms. The approved business models for the firms differ, and the firms are approved to engage in those activities enumerated in OCC approval letters.[145]

Two states—New York and Wyoming—have established frameworks in which crypto firms may obtain special state banking charters. In New York, firms may apply for limited purpose trust company charters.[146] The application includes filing a business plan with the New York State Department of Financial Services and holding surety bonds, among other requirements.[147] Like the BitLicense, another New York–specific crypto firm designation, the state's special purpose charter allows an institution to conduct a virtual currency business. It also provides additional "benefits" including permission to "exercise fiduciary powers" and to engage in money

[141] See CFTC, "Bitcoin Basics," https://www.cftc.gov/sites/default/files/2019-12/oceo_Bitcoinbasics0218.pdf; and LabCFTC, *A CFTC Primer on Virtual Currencies*, October 17, 2017, https://www.cftc.gov/sites/default/files/idc/groups/public/documents/file/labcftc_primercurrencies100417.pdf.

[142] Benjamin W. McDonough, *Interpretive Letter #1179, November 2021: 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*, OCC, November 18, 2021, https://www.occ.gov/topics/charters-and-licensing/interpretations-and-actions/2021/int1179.pdf.

[143] McDonough, *Interpretive Letter #1179, November 2021*. At around the same time, the bank regulators, consisting of the OCC, the Federal Reserve, and the Federal Deposit Insurance Corporation issued a notice that they had participated in a crypto-asset sprint and would continue to provide guidance regarding banks' ability to engage in various crypto activities. See Board of Governors of the Federal Reserve System, Federal Deposit Insurance Corporation, OCC, "Joint Statement on Crypto-Asset Policy Sprint Initiative and Next Steps," November 23, 2021, https://www.occ.gov/news-issuances/news-releases/2021/nr-ia-2021-120a.pdf.

[144] Jonathan V. Gould, *Interpretive Letter #1176, Chief Counsel's Interpretation on National Trust Banks*, OCC, January 11, 2021, https://www.occ.gov/topics/charters-and-licensing/interpretations-and-actions/2021/int1176.pdf; and McDonough, *Interpretive Letter #1179, November 2021*.

[145] For a complete discussion of state and national bank engage in crypto activities, see CRS In Focus IF11997, *Bank Custody, Trust Banks, and Cryptocurrency*, by Andrew P. Scott.

[146] New York State Department of Financial Services, "Virtual Currency Businesses," https://www.dfs.ny.gov/virtual_currency_businesses; and "Banks and Trusts," https://www.dfs.ny.gov/apps_and_licensing/banks_and_trusts/commercial_banks_trusts.

[147] New York State Department of Financial Services, "Commercial Banks and Trust Companies," https://www.dfs.ny.gov/apps_and_licensing/banks_and_trusts/commercial_banks_trusts.

transmission without an additional license.[148] Institutions with limited purpose trust company charters in New York include Coinbase Custody Trust, Paxos Trust Company, and NYDIG Trust Company, among several others.[149] Limited purpose trust companies do not accept deposits and are not insured by the Federal Deposit Insurance Corporation.[150]

Wyoming's charter is called a special purpose depository institution (SPDI). SPDIs are "banks that receive deposits and conduct other activity incidental to the business of banking, including custody, asset servicing, fiduciary asset management, and related activities."[151] The Wyoming Division of Banking has suggested that SPDIs are likely to focus on digital assets but can also operate in traditional asset and cash management and engage in other purposes permitted under applicable law. SPDIs are prohibited from making loans with customer deposits of fiat currency and must hold certain high-quality liquid assets with a value of at least 100% of depository liabilities.[152]

Applicable Money Services Businesses Framework

Cryptocurrency exchanges often register as money services businesses (MSBs) in order to operate. The regulatory framework for MSBs is largely a state-based licensing regime and applies to many nonbank institutions, including several crypto-related companies, such as cryptocurrency trading platforms, payment platforms that allow customers to buy and hold cryptocurrency, and automated teller machines (ATMs) that sell or allow the transfer of cryptocurrencies.[153] However, specific approaches to include crypto in MSB regulation vary by state. For instance, some states have created additional programs (e.g., New York's BitLicense), while others (e.g., Wyoming) have exempted digital currency businesses from MSB regulation altogether.[154] Moreover, the supervisory programs (exam frequency, the depth and breadth of exams, and dedicated resources) vary considerably by state.

At the federal level, these crypto firms (exchanges, payment platforms, ATMs) are considered MSBs and must register with the Financial Crimes Enforcement Network.[155] As such, they must comply with AML laws. Among other things, those laws require financial institutions to establish customer identification programs and abide by certain reporting and recordkeeping requirements.[156] FinCEN is not a regulator, however, so registration with FinCEN does not subject crypto firms to federal regulation outside of AML compliance.

---

[148] New York State Department of Financial Services, "Virtual Currency Businesses." The BitLicense is a New York State designation required of companies that wish to engage in virtual currency exchange.

[149] New York State Department of Financial Services, "Virtual Currency Businesses."

[150] New York State Department of Financial Services, "Banking Interpretations," https://www.dfs.ny.gov/legal/interpret/lo060216a.htm.

[151] Wyoming Division of Banking, "Special Purpose Depository Institutions," https://wyomingbankingdivision.wyo.gov/banks-and-trust-companies/special-purpose-depository-institutions.

[152] Wyoming Division of Banking, "Special Purpose Depository Institutions."

[153] Exchanges may seek money transmitter licenses based on state law or convention. For a state-by-state overview of regulations, see *Bloomberg Law*, "Cryptocurrency Laws and Regulations by State," May 26, 2022, https://pro.bloomberglaw.com/brief/cryptocurrency-laws-and-regulations-by-state/.

[154] *Bloomberg Law*, "Cryptocurrency Laws and Regulations by State." For New York's BitLicense, see https://www.dfs.ny.gov/virtual_currency_businesses; and for Wyoming, see https://law.justia.com/codes/wyoming/2021/title-40/chapter-22/section-40-22-104/.

[155] FinCEN, *FinCEN Guidance: Application of FinCEN's Regulations to Certain Business Models*.

[156] For a deeper look at how MSBs are regulated and some policy issues around the regulation of digital asset exchanges, see CRS Report R46486, *Telegraphs, Steamships, and Virtual Currency: An Analysis of Money Transmitter*

The Future of Cryptocurrency Regulation

There appears to be a growing consensus among domestic and international policymakers of the need for greater clarity and coordination and new regulation. In its annual report for 2021, the Financial Stability Oversight Council (FSOC) noted that "regulatory attention and coordination are critically important in light of the quickly evolving market for these assets."[157] Lael Brainard, the vice chair of the Board of Governors of the Federal Reserve System, highlighted in a July 2022 speech that despite the novelty, the "crypto financial system turns out to be susceptible to the same risks that are all too familiar from traditional finance" and that regulators should include digital assets in the "regulatory perimeter."[158] The Financial Stability Board expressed similar concerns in the international domain, noting that "the rapid evolution and international nature of these markets also raise the potential for regulatory gaps, fragmentation or arbitrage."[159] It continued that while the industry is not so large and interconnected with traditional finance to create stability concerns now, it is appropriate "to ensure that like risks are subject to like regulatory outcomes." Most recently, an FSOC report published pursuant to the President's executive order noted that "large parts of the crypto-asset ecosystem are covered by the existing regulatory structure" and that it "emphasizes the importance of continued enforcement of existing rules and regulations."[160] Nevertheless, it identified what FSOC sees as various gaps, including limited federal oversight of spot markets and opportunities for regulatory arbitrage, among others, and called for legislation to empower regulators to address these gaps.[161]

Calls for greater regulation of the industry preceded the November 2022 collapse of FTX, a prominent cryptocurrency trading platform. While it is unclear whether stricter regulations may have prevented the situation at FTX, which was a Bahamas-based entity, AML statutes have been applied to companies in foreign jurisdictions when the proceeds of illegal activity were included in banking transactions that cleared in the United States. U.S. regulations may also apply if the company actively sought customers in the United States.

Regardless of jurisdiction, the events at FTX are relevant because they shine a light on practices by U.S.-based exchanges that may be of interest to Congress. The first is whether and how these firms—many of which are not registered as traditional securities exchanges and therefore are not subject to the same regulatory framework as traditional exchanges—should be regulated. In addition, most cryptocurrency exchanges currently operate concurrently as (1) exchanges, providing a platform on which their customers can buy and sell; (2) broker-dealers, in which role they are themselves the buyers and sellers; and (3) custodians, providing custody services for their customers. Moreover, some exchanges are partners in issuing stablecoins, which may then be traded on exchanges, some of which cannot be directly redeemed. This is counter to how traditional exchanges, which are neutral and do not take positions, operate.[162] Policymakers and

Regulation, by Andrew P. Scott.

[157] FSOC, *2021 Annual Report*, December 17, 2021, p. 17, https://home.treasury.gov/system/files/261/FSOC2021AnnualReport.pdf.

[158] Lael Brainard, "Crypto-Assets and Decentralized Finance Through a Financial Stability Lens," Bank of England Conference, July 8, 2022, https://www.federalreserve.gov/newsevents/speech/brainard20220708a.htm.

[159] Financial Stability Board, *Assessment of Risks to Financial Stability from Crypto-Assets*, February 16, 2022, p. 1, https://www.fsb.org/wp-content/uploads/P160222.pdf.

[160] FSOC, *Report on Digital Asset Financial Stability Risks and Regulation*, October 3, 2022, p. 111, https://home.treasury.gov/system/files/261/FSOC-Digital-Assets-Report-2022.pdf.

[161] FSOC, *Report on Digital Asset Financial Stability Risks and Regulation*.

[162] See Craig Pirrong quote in Kaminska, "Why Coinbase's Stellar Earnings Are Not What They Seem."

other observers have argued that playing these multiple roles simultaneously may pose conflicts of interest.[163]

Unlike traditional brokers, which must segregate customer funds, crypto exchanges may have comingled funds, making it difficult for customers to recover funds if the exchange were hacked or went bankrupt. As such, Congress may choose to require that they segregate customer funds.

Additional policy issues can be summed up in three, still-unanswered policy questions. First, is the current authority sufficient and clear, or does the environment require congressional action? There is lack of consensus on this first issue. While the SEC has repeatedly expressed the belief that existing laws are sufficient, there are areas where the CFTC believes additional authorization is required.[164] The other two policy questions are closely intertwined: Assuming broad new regulatory authority is required, is it better to create a new, overarching structure, or is a refinement of the existing framework sufficient? If the current framework is refined, who should have authority?

Congress may choose to establish some rubric that distinguishes digital asset commodities from securities and create procedures for registering the two types of digital assets and their respective exchanges. Congress may consider amending the definitions of *commodity* or *security* to accommodate certain types of digital assets, as there appears to be a lack of consensus among regulators. It may also decide to designate new terms for assets that it believes fall outside existing frameworks. For example, legislation could require that one type of asset fall under the primary jurisdiction of one regulator while also assigning specific responsibilities to another regulator.[165] Such legislation may distinguish digital commodities that were available to certain investors before they were publicly available from those that were not and use that or some other trait as a factor in designating the primary regulator.

Congress may choose to expand the authority of the CFTC or SEC or encourage them to engage in rulemaking using their existing authorities. As the stickiest issue appears to be determining whether one of thousands of cryptocurrencies that may be traded is a commodity or security, requiring the CFTC and SEC to deliberate collectively on the classification of newly listed digital assets may help provide clarity. Finally, additional regulatory requirements are likely to create new responsibilities for agencies, and Congress may choose to provide additional funding to either or both of the agencies depending on how mandates change.[166]

Beyond the practical discussion of who should be the primary regulator and which regulatory framework applies in which set of circumstances, there are issues that are perhaps even more fundamental. The lack of an overarching regulatory framework with clear delineations can be awkward, because in the absence of clear rules of the road, less-informed participants may assume that the products have a stamp of approval when they do not. Alternatively, from an industry perspective, regulatory ambiguity creates the potential for sudden shifts in the regulatory landscape that may hinder current industry activities or offerings. While the discussion in this section has thus far been limited to the regulation of relatively new crypto entities, policymakers

[163] Gensler, *Kennedy and Crypto*; and Gary Gensler, *Prepared Remarks of Gary Gensler on Crypto Markets Penn Law Capital Markets Association Annual Conference*.

[164] For example, Gensler believes the securities framework is sufficient. Benham believes his agency requires explicit congressional authority in at least one area: commodity token spot markets. See footnote 119 above for sources.

[165] According to one bill, an "ancillary asset" would be under the jurisdiction of the CFTC but would have disclosure reporting requirements with the SEC.

[166] Jennifer Schonberger, "SEC's Gensler: The 'Runway Is Getting Shorter' for Non-Compliant Crypto Firms," *Yahoo Finance*, December 7, 2022, https://finance.yahoo.com/video/sec-gensler-runway-getting-shorter-161605453.html.

may also ask whether crypto activities should be available to traditional financial institutions or whether there should be any required separations. Both cases—establishing clear rules and providing an avenue to integrate with traditional finance—may also confer a level of legitimacy some observers do not believe the crypto industry deserves and create systemic risk no one is likely to want.

Tax Implications

The Internal Revenue Service treats cryptocurrency as property for tax purposes.[167] This means that receipt of crypto as a form of payment, and the sale or exchange of crypto, may have tax consequences.[168] Whether the resulting income (or loss) from a transaction involving crypto is characterized as capital or ordinary income would depend on how such assets were being used.[169] For example, crypto received in exchange for a service would be categorized as ordinary income, and the taxpayer would include the fair market value of the crypto received when computing gross income.[170] Alternatively, when crypto is exchanged for another asset or converted into fiat currency (e.g., dollars), the transaction would result in a capital gain or loss.[171] The amount of the gain or loss would depend on fair market value of the asset received and the taxpayer's "basis" in the crypto (which is generally the fair market value of the crypto at the time of the transaction).[172] Because cryptocurrencies are not widely accepted for day-to-day payments, cryptocurrency owners must often convert their cryptocurrency into fiat currency before it can be used. That conversion would typically constitute a taxable event.[173]

The Infrastructure Investment and Jobs Act (P.L. 117-58) imposes additional data reporting requirements for brokers. Brokers must provide returns (1099-B) for taxpayers' trades performed on their platforms.[174] The law also requires that individuals and companies who receive more than $10,000 in crypto proceeds from a single transaction in the course of their trade or business file returns with respect to the transaction.[175] Such information must include the identity of the sender.[176]

---

[167] Internal Revenue Service (IRS), "Frequently Asked Questions on Virtual Currency Transactions," https://www.irs.gov/individuals/international-taxpayers/frequently-asked-questions-on-virtual-currency-transactions.

[168] IRS, "Digital Assets," https://www.irs.gov/businesses/small-businesses-self-employed/digital-assets.

[169] IRS, *LB&I International Practice Service Concept Unit*, p. 3, https://www.irs.gov/pub/int_practice_units/fcu_cu_c_18_2_1_04.pdf; IRS, *Notice 2014-21: IRS Virtual Currency Guidance*, April 14, 2014, https://www.irs.gov/irb/2014-16_IRB#NOT-2014-21; and IRS, *Publication 544: Sales and Other Dispositions of Asset*, February 16, 2022, https://www.irs.gov/pub/irs-pdf/p544.pdf.

[170] IRS, "Frequently Asked Questions on Virtual Currency Transactions."

[171] IRS, "Frequently Asked Questions on Virtual Currency Transactions." There are many caveats to this. First, presumably, the person is not a dealer, and second, the person must hold the asset for the holding period, etc.

[172] IRS, "Frequently Asked Questions on Virtual Currency Transactions."

[173] IRS, "Frequently Asked Questions on Virtual Currency Transactions."

[174] See CRS In Focus IF11910, *Cryptocurrency Transfers and Data Collection*, by Mark P. Keightley and Andrew P. Scott; and Laura Davison, "How Taxing Crypto Got Changed by Biden's Infrastructure Law," *Bloomberg*, November 17, 2021), https://www.bloomberg.com/news/articles/2021-11-17/how-taxing-crypto-got-changed-by-infrastructure-law-quicktake. Soon after the law was signed, various Members of Congress expressed interest in altering the definition of *broker* to omit software developers, miners, and various other parties.

[175] 26 U.S.C. §6050I.

[176] Davison, "How Taxing Crypto Got Changed by Biden's Infrastructure Law." This would be reported on Form 8300. Tim Shaw, "The Long Read: Catching Up with Crypto," *Thompson Reuters*, April 29, 2022, https://tax.thomsonreuters.com/news/the-long-read-catching-up-with-crypto/.

Energy Intensity[177]

The energy-intensive nature of the technology and process underpinning the cryptocurrency ecosystem has emerged as a key policy issue. This section aims to introduce some of the issues. For a comprehensive look at crypto energy intensity and attendant environmental concerns, see CRS Report R45863, *Bitcoin, Blockchain, and the Energy Sector*, by Corrie E. Clark and Heather L. Greenley.

As discussed above ("Blockchain, Decentralized Consensus, and Cryptography") the proof of work consensus mechanism is a key design feature that secures the network and maintains the integrity of the distributed ledger for certain cryptocurrencies. It requires that mining nodes engage in computationally complex processes that require sophisticated computers and significant amounts of energy. In addition, the hardware performing these functions can generate significant heat and demand significant amounts of energy to cool the equipment. Various factors contribute to the amount of energy consumption used in mining, including the type of hardware computing power, the network hashrate, the difficulty of proof of work calculations, and the thermal regulation of the hardware.[178] Recent estimates of the amount of energy used by the Bitcoin network alone is about 82.5 terawatt hours, or roughly equivalent to the amount of energy used by the country of Belgium in one year.[179]

President Biden's Executive Order 14067 directed the White House Office of Science and Technology Policy and its partners to prepare a report that, among other things, would examine "the potential for these technologies to impede or advance efforts to tackle climate change at home and abroad; and the impacts these technologies have on the environment."[180]

The resulting report has various general recommendations, which include improving collection of data, encouraging mining companies to report their locations, improving environmental performance of equipment, and supporting research and development that would improve the "environmental sustainability of digital assets, including crypto-assets," among others.[181] The report recommends that various stakeholders try to devise more environmentally responsible crypto technologies. If interventions to reduce energy use fail, the report recommends the Administration use executive action and suggests that Congress "might consider" legislation to "eliminate the use of high energy intensity consensus mechanisms for crypto-asset mining."[182] The report also urges the Administration to work with Congress, the Department of Energy, and other agencies to "promulgate and regularly update energy conservation standards for crypto-asset mining equipment, blockchains, and other operations."

---

[177] For an in-depth look at environmental issues related to cryptocurrency, see CRS Report R45863, *Bitcoin, Blockchain, and the Energy Sector*, by Corrie E. Clark and Heather L. Greenley; and CRS In Focus IF12286, *Recent Cryptocurrency Developments: Energy and Environmental Implications*, by Kristen E. Busch and Corrie E. Clark.

[178] For more information on energy and environmental-related policy options for cryptocurrency mining, see CRS Report R45863, *Bitcoin, Blockchain, and the Energy Sector*, by Corrie E. Clark and Heather L. Greenley.

[179] University of Cambridge Judge Business School Centre for Alternative Finance, "Cambridge Bitcoin Electricity Consumption Index," at https://ccaf.io/cbeci/index/comparisons. Consumption changes regularly, as do country comparisons.

[180] E.O. 14067.

[181] White House Office of Science and Technology Policy, *Climate and Energy Implications of Crypto-Assets in the United States*, September 8, 2022, https://www.whitehouse.gov/wp-content/uploads/2022/09/09-2022-Crypto-Assets-and-Climate-Report.pdf.

[182] White House Office of Science and Technology Policy, *Climate and Energy Implications of Crypto-Assets in the United States*.

Some market participants have committed to undertaking a shift to less energy-intensive consensus protocols, such as proof of stake (see "Ethereum").[183]

Outlook

Cryptocurrencies will likely continue to be of interest in the 118th Congress. Price volatility is likely to create gains for some and losses for others. More failures of exchanges or platforms cannot be ruled out, potentially leading to large losses for some and destabilizing the industry generally. Unsophisticated investors, drawn by promises of big payouts without understanding the instruments or their risks, might be especially vulnerable. Overall, market developments are highly uncertain and may merit close monitoring by policymakers. Congress faces options for oversight and legislation that may aim to make significant changes to the regulatory framework applied to crypto.

Author Information

Paul Tierno
Analyst in Financial Economics

Disclaimer

This document was prepared by the Congressional Research Service (CRS). CRS serves as nonpartisan shared staff to congressional committees and Members of Congress. It operates solely at the behest of and under the direction of Congress. Information in a CRS Report should not be relied upon for purposes other than public understanding of information that has been provided by CRS to Members of Congress in connection with CRS's institutional role. CRS Reports, as a work of the United States Government, are not subject to copyright protection in the United States. Any CRS Report may be reproduced and distributed in its entirety without permission from CRS. However, as a CRS Report may include copyrighted images or material from a third party, you may need to obtain the permission of the copyright holder if you wish to copy or otherwise use copyrighted material.

[183] Under the proof of stake consensus mechanism, "validators"—the name given to node operators who take the place of miners from the proof of work consensus model—do not compete for the ability to mine a block, but they are selected to validate transactions. This mechanism dispenses with the complex cryptographic calculations and the associated hardware and energy needs. Instead, validators stake their holdings for the opportunity to generate more.