Introduction to Cryptocurrency

Cryptocurrencies (or *crypto*) are digital assets exchanged and recorded on public distributed ledgers (known as *blockchains*) that do not require central intermediaries (e.g., commercial banks, central banks) for clearing and settlement. Transactions are public and users are pseudonymous, so, while transactions are visible to all, users, whose pseudonyms bear no connection to their true identities, enjoy a level of secrecy. Initially introduced as payments tools, cryptocurrencies are mostly used as a form of investment. This In Focus introduces crypto market structure, regulatory frameworks, and policy issues. For more information, see CRS Report R47425, *Cryptocurrency: Selected Policy Issues*.

Cryptocurrencies: An Overview
Once used by a small subset of computer scientists, crypto has gone global. Crypto has experienced continual, rapid growth and significant price fluctuations. Between 2021 and 2022, after reaching what was then an all-time high of around $3 trillion, the market lost two-thirds of its value and fell to $800 billion. Since then, the market increased steeply again and is currently valued at $3.46 trillion.

Crypto attempts to replace the trust-based traditional financial system with one that does not require trust. In lieu of traditional financial regulatory staples such as chartering, supervision, and deposit insurance, the cryptocurrency system leverages cryptography and a series of separate but concurrent incentives for different system participants, such as mining and block rewards.

In recent years, large financial intermediaries—the very type of institutions crypto developers sought to obviate—have displaced the decentralized, trustless ideal. For example, crypto was originally accessible via less-than-user-friendly blockchains, but more user-friendly and familiar systems have been created, allowing individuals and firms to "custody" their crypto in accounts or "wallets" at institutions. An entire ecosystem has developed that supports cryptocurrencies, including the custody or hosting services known as wallets, as well as exchanges, payment platforms, decentralized finance platforms, and more.

Transacting with Crypto
Users may interact with crypto via *on-chain* transactions, which are processed over a blockchain, a network of nodes that maintain the system. Users send and receive cryptocurrency on-chain using *unhosted* wallets that store the keys that secure ownership of and permit transaction of crypto. Assets on a blockchain are protected by *asymmetric key cryptography*, which encrypts and protects data.

Off-chain transactions occur outside of blockchains. Instead, they are generally facilitated, processed, and recorded by online platforms, such as crypto exchanges, which host users' *custodial* or *hosted wallets*. Exchanges allow users to exchange fiat currency into crypto and vice versa. These platforms allow users to trade digital assets, make markets for various assets, and offer other services.

Types of Cryptocurrencies
The two most widely used cryptocurrencies are Bitcoin and Ether, which, as of January 2025, represent more than 65% of the crypto market capitalization. *Bitcoin* was the first cryptocurrency to gain widespread popularity. In Bitcoin, *decentralized consensus mechanisms* encourage some network participants (called miners) to secure the system for financial gain. Bitcoin relies on a *proof of work (PoW)* consensus mechanism that rewards miners with greater computational resources and cheaper energy sources.

Ether is the cryptocurrency native to the Ethereum blockchain. Unlike Bitcoin, Ether uses *proof of stake (PoS)*, a less energy-intensive consensus mechanism than PoW. In PoS, computational effort of PoW is replaced with collateral: Validators lock or "stake" at least 32 Ether to enter a pool to be given a chance to validate the next block. The network may seize collateral for malicious activity or other offenses. Ethereum also enables smart contracts, which are applications that self-execute when participants meet some predetermined set of criteria. Because of the enhanced programmability, Ethereum is widely used for decentralized finance (or *DeFi*) projects that aim to mimic traditional finance but without intermediaries.

Stablecoins
Cryptocurrencies such as Bitcoin and Ether fluctuate in value based on market supply and demand. By contrast, stablecoins are "designed to maintain a stable value relative to a national currency or other … assets." For example, the Tether and USDC stablecoins are set equal in value to $1. Total market capitalization for stablecoins is greater than $200 billion. As with cryptocurrencies, stablecoins are not generally accepted for retail payments and are primarily used when trading crypto. Stablecoins may attempt to match their value to equivalent fiat currencies in different ways but have been known to lose their stable values. For more, see CRS In Focus IF11968, *Stablecoins: Background and Policy Issues*.

Central Bank Digital Currency
The premise of central bank digital currencies (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. For example, CBDCs could be used for payments, much the way crypto was intended. However, CBDCs would be legal tender and exist as dollars themselves instead of having

values linked to dollars. Currently, there are no plans for a U.S. CBDC, but other countries have introduced or are in the process of introducing their own. For more, see CRS In Focus IF11471, *Central Bank Digital Currencies*.

Crypto Regulation

There is no comprehensive regulatory framework for crypto, and regulators have issued few rules specific to crypto. In the absence of an overarching framework, regulators may apply existing regulatory frameworks as circumstances dictate. It is possible that crypto may be subject to various existing regulatory frameworks depending in part on regulatory interpretation, the specific crypto product, how it is used, and what it is used for.

Applicable SEC Framework

Some policymakers believe that "many of the tokens trading on these [crypto trading] platforms may well meet the definition of 'securities,'" which would require both the tokens and platforms to register with the Securities and Exchange Commission (SEC) and become subject to SEC regulation, absent an exemption. In several cases, the SEC has used the *Howey test* to determine whether cryptocurrencies qualify as securities. Under that test, an instrument is deemed an "investment contact" (a category of security) if it involves (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. For more, see CRS Report R46208, *Digital Assets and SEC Regulation*.

Applicable CFTC Framework

The Commodity Futures Trading Commission (CFTC) administers the Commodity Exchange Act, which defines *commodities* as various agricultural products and natural resources—such as gold, oil, wheat, and cotton—as well as services and rights in which futures may be dealt. In 2015 the agency brought an enforcement action against a Bitcoin options and futures platform, concluding that Bitcoin and other virtual currencies are "commodities." Various federal court decisions have since supported the CFTC's position that the act's definition of the term *commodity* encompasses virtual currency. Entities offering trading of crypto futures and options must register with the CFTC, whose authority in spot (cash) markets is limited to enforcing prohibitions on fraud and manipulation.

Applicable Banking Framework

Bank involvement with crypto can fall into three categories. First, banks can provide traditional banking services, such as lending and deposit taking, to crypto firms. Second, banks can provide crypto services, such as payment applications and tokenization. Third, crypto firms can seek to acquire banks or bank charters. Federal bank involvement in crypto activities faces a two-prong regulatory test. First, an activity must be permissible under law—Congress has limited banks' activities related or incidental to the business of banking. Second, an activity must be safe and sound.

Crypto firms may seek federal bank charters from the Office of the Comptroller of the Currency to provide limited crypto services. Various states, including New York and Wyoming, have established frameworks in which crypto firms may obtain special state banking charters. For more information, see CRS In Focus IF12320, *Crypto and Banking: Policy Issues*.

Applicable Money Services Business 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, including exchanges and crypto automated teller machines. At the federal level, these crypto firms are considered MSBs and must register with the Financial Crimes Enforcement Network and comply with the Bank Secrecy Act and implement anti-money laundering (AML) and know-your-customer (KYC) programs. For more, see CRS Report R46486, *Telegraphs, Steamships, and Virtual Currency: An Analysis of Money Transmitter Regulation*.

Selected Policy Issues

Congress is divided on whether policy should foster, ignore, or quarantine the crypto industry, raising some policy issues. Policymakers generally debate how to cultivate innovation while minimizing crypto's potential harms.

Future of regulation. Traditional financial institutions are subject to an array of regulations, such as prudential standards and disclosure requirements. Historically, the crypto industry has exhibited non-compliance with and uneven enforcement of applicable frameworks. Potential future crypto regulation may choose to implement rules that resemble the traditional financial system.

The regulatory policy debate has focused on whether a regulatory regime that is tailored for crypto is necessary. Other key policy issues can be summed up in three unanswered questions: Are current regulatory authorities sufficient, or is congressional action required? If new regulatory authority is required, who should be the primary regulator? Is it better to create a new, overarching structure, or is a refinement of the existing framework sufficient?

Several bills regarding crypto were introduced in the 118th Congress addressing these issues. They include House-passed H.R. 4763, the Financial Innovation and Technology for the 21st Century Act, and H.R. 4766, the Clarity for Payment Stablecoins Act of 2023.

Privacy vs. illicit activity. The same characteristics that address a legitimate desire for privacy also provides secrecy that makes it useful for engaging in illicit activity. Balancing the potential privacy provided by crypto's pseudonymity with the requirement that financial firms comply with AML/KYC programs is a key policy issue.

Energy and the environment. The Bitcoin network's annual energy consumption has recently been estimated to be about 180 terawatt hours, or somewhat more than the amount of energy used by Egypt. For more, see CRS Report R45863, *Bitcoin, Blockchain, and the Energy Sector*.

Consumer and investor protection. Some argue that numerous scams and frauds—embodied by the 2022 collapse of crypto firm FTX—highlight a lack of investor and consumer protections in the industry.

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.