



May 23, 2023

Introduction to Cryptocurrency

Cryptocurrencies (or *crypto*) are digital financial instruments exchanged and recorded on public ledgers (known as *blockchains*) that do not require central intermediaries (e.g., commercial banks, central banks) for clearing and settlement. Users and transactions are public but pseudonymous, which means users' identities may be obscured. 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, see CRS Report R47425, *Cryptocurrency: Selected Policy Issues*, and CRS Report R47064, *Blockchain: Novel Provenance Applications*.

Cryptocurrencies: An Overview

Once used by a small subset of computer scientists, crypto has gone global. Crypto has been characterized by continual and rapid price increases and decreases. Recently, after experiencing dramatic growth that propelled it to a record high of around \$3 trillion in November 2021, the market capitalization fell to less than \$800 billion in November 2022 in what has been referred to as a “crypto winter.” As of May 2023, it is valued at around \$1.1 trillion.

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, such as 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.

In recent years, large financial intermediaries—the very type of institutions crypto wanted to make unnecessary—have displaced the decentralized, trustless ideal. 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. 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.

Transacting with Crypto

On-chain transactions are transactions processed over the blockchain, the 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 uses a *public key* to encrypt and a *private key* to decrypt data.

Off-chain transactions are any transactions that occur outside of the main blockchains. Instead, they are generally facilitated, processed, and recorded by online platforms, such as crypto exchanges (e.g., Binance, Coinbase), 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 May 2023, represent more than 60% of the crypto market capitalization. *Bitcoin* was the first cryptocurrency to gain widespread adoption. Bitcoin functions as a unit of account and medium of exchange. 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 who possess greater computational resources and energy demands.

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 digital assets “designed to maintain a stable value relative to a national currency or other reference assets.” For example, the Tether and USD Coin (USDC) stablecoins are set equal in value to \$1. Total market capitalization for stablecoins is greater than \$130 billion. As with cryptocurrencies, stablecoins are not generally accepted for payment 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 designed to be linked to dollars. For more, see CRS In Focus IF11471, *Central Bank Digital Currencies*.

Crypto Regulation

Currently, there is no comprehensive regulatory framework for crypto, but regulators may apply existing regulatory frameworks when applicable to crypto.

Applicable SEC Framework

In an April 2022 speech, Gary Gensler, chair of the Securities and Exchange Commission (SEC), stated that “many of the tokens trading on these [crypto trading and lending platforms] may well meet the definition of ‘securities.’” If so, both the tokens and platforms are required to register with the SEC and become subject to SEC regulation. 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. 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—such as wheat and cotton, among others—as well as services and rights in which futures may be dealt. Using this definition, 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 Commodity Exchange 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

Various states, including New York and Wyoming, have established frameworks in which crypto firms may obtain special state banking charters. At the federal level, national banks can seek approval from the Office of the Comptroller of the Currency to provide limited crypto services, such as crypto custody services, holding reserves, and using node verification networks and stablecoin for payments. In addition, a crypto firm may seek a national bank trust charter, which limits the holder to “fiduciary capacity” operations permitted by federal statute and laws in the trust bank or company’s home state. Firms with bank charters become subject to federal bank regulation. For more, 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, such as trading platforms, payment platforms, and crypto automated teller machines. At the federal level, these various 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

The relative novelty of how cryptocurrency transactions occur introduces a host of policy issues.

Privacy vs. illicit activity: The same characteristics that make crypto a favorite of users with a legitimate desire for privacy also provides secrecy that may make it useful for engaging in illicit activity. Balancing the potential privacy provided by crypto’s pseudonymity with the requirement that financial firms comply AML/KYC programs is as a key policy issue.

Energy and the environment: The PoW consensus mechanism used by some cryptocurrencies requires use of sophisticated computers and significant amounts of energy to power and cool the equipment. Recent estimates of the Bitcoin network’s annual energy consumption put the amount at about 147 terawatt hours, or roughly equivalent to the amount of energy used by Malaysia. In light of this issue, some market participants have shifted to the less energy-intensive PoS consensus protocol. Moreover, various federal agencies are examining the impacts these technologies have on the environment. For more, see CRS Report R45863, *Bitcoin, Blockchain, and the Energy Sector*.

Future of regulation: Traditional financial institutions are subject to an array of regulations, such as prudential standards or disclosures requirements. In the crypto industry, on the other hand, non-compliance with and uneven enforcement of applicable frameworks has created the impression that the industry is not subject to those rules or is breaking them. Potential future crypto regulation may choose to require disclosure, segregation of customer funds, and limitations on platforms’ tendency to play multiple roles simultaneously that some say lead to conflicts of interest—all of which are required in traditional finance.

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: Is the current authority 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?

Consumer and investor protection: Some argue that numerous scams and frauds—recently embodied by the collapse of FTX—highlight a lack of investment 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.