GEORGETOWN UNIVERSITY
Psaros Center for Financial Markets and Policy
McDONOUGH SCHOOL of BUSINESS

Decrypting Crypto: Cryptocurrency

Edited by Yaya J. Fanusie, Visiting Fellow
Written by Michelle Chen and Ana Mocanu, Research Assistants

Key Insight

Cryptocurrencies have introduced a new way to transmit value on the internet, prompting traditional financial institutions to explore ways to integrate the technology into mainstream use. The regulatory environment still faces significant regulatory uncertainty in the United States, but the European Union has taken major steps to formalize its cryptocurrency markets.

Summary

Cryptocurrencies are units of digital ownership recorded on a distributed ledger system known as a **blockchain**. Unlike fiat currencies issued by national governments that need regulated financial institutions to facilitate digital transactions, cryptocurrencies run on public blockchain platforms where a transaction settlement is conducted by a network of computers open to anyone with internet access.

Cryptocurrency transactions occur directly between individual wallets and are verified by a decentralized network of validators or miners, who confirm the transactions in batches before adding them to the blockchain. This approach makes the entire transaction history of all wallets publicly visible without requiring or attaching users' personal identification to the wallets.

Key Facts

To own cryptocurrency and transact on a blockchain, one must have a private key: a unique string of numbers and characters tying specific units of data on the blockchain to a digital wallet. Similar to the function of physical wallets, digital wallets can store one's private funds as well as credentials for transacting. They fall under two general categories, custodial and self-custodial, with the former being more widely adopted by the casual user.

A custodial wallet's private keys are managed by a firm on behalf of the user. Access to cryptocurrency accounts is primarily verified through traditional passwords and biometric verification processes. Examples of such custodians include Coinbase, Binance, and Blockchain.com.

A self-custodial wallet keeps the private key with the user, giving the users full control of the wallet's contents. While this keeps funds more secure from hacks, self-custodial wallets tend to be less user-friendly than custodial wallets and require more diligence in protecting one's private key.

Some businesses do accept cryptocurrency payment methods, but it is not widespread. A study estimated that around 2,352 US businesses accept Bitcoin. One noteworthy case is U.S. Telecom provider AT&T, which began accepting payments in 2019 through cryptocurrency payment processor BitPay. In

2021, $1.2 trillion was exchanged in conventional banking cross-border payments. Cryptocurrency is borderless with users generally able to transact with anyone with a corresponding crypto wallet. This ease of access offers potential opportunities for improving financial efficiency and access.

Key Institutions

Developers, validators, and miners form the backbone of the cryptocurrency ecosystem, designing blockchain **protocols** and verifying transactions to maintain system integrity. While cryptocurrency trading was initially limited to a niche group of technologists, it has become increasingly accessible to the general public through exchanges and regulated products. Centralized exchanges like Binance, Coinbase, and Kraken simplify trading with user-friendly interfaces, fiat on-ramps, and services like staking and lending, lowering barriers to entry for retail investors. Simultaneously, institutional players like Grayscale, BlackRock, and Fidelity are introducing regulated products such as Spot Bitcoin and Ethereum ETFs, broadening access and seeking to integrate crypto into mainstream finance. Technology companies and payment processors like Block and Paypal have been developing end-market applications integrating crypto with day-to-day payment transactions. These activities occur within a still-evolving policy environment, where regulators are tasked with helping the cryptocurrency sector balance innovation with consumer protection, addressing risks such as money laundering and market manipulation.

Background

The roots of digital currency systems trace back to the late twentieth century, beginning with David Chaum's DigiCash in 1983. DigiCash introduced cryptographic protocols as a way to secure digital transactions and enable anonymous payments.

However, it relied on a centralized structure, which limited its potential and scalability by creating decision-making bottlenecks and limiting adaptability to market changes. Later, in 1998, Wei Dai proposed the concept of a pseudonymous electronic cash system called b-money, while Nick Szabo developed the framework for another cryptographic digital transaction system called Bit Gold. Though never fully implemented, both were among the earliest and most impactful attempts to create decentralized virtual currencies. They introduced foundational concepts such as distributed ledgers, proof-of-work, and anonymous transactions, laying the groundwork for the eventual development of Bitcoin's protocol.

Bitcoin, the first and still most popular cryptocurrency, was introduced in 2009 by the pseudonymous creator Satoshi Nakamoto. Its biggest breakthrough was establishing a system where users could trust the validity of online transactions without relying on a central authority. Unlike previous attempts at internet-based currency, Bitcoin successfully implemented a proof-of-work system where computers seek rewards by racing to solve cryptographic puzzles. This incentivizes validators to participate in the confirmation transaction process and thus maintain network integrity, solving the **double-spending problem** (use of the same token to conduct multiple transactions). Bitcoin's supply is fixed at 21 million coins, creating scarcity, and each bitcoin can be broken down into smaller units, a divisibility allowing Bitcoin to function as an exchange medium even when its value increases. Bitcoin proponents argue that this scarcity positions it as a hedge against inflation. Moreover, Bitcoin's popularity was not only due to technological innovation but also its timing, offering a decentralized alternative during a global financial crisis that provoked dissatisfaction with traditional financial systems.

Today, the cryptocurrency market has grown, encompassing thousands of coins beyond Bitcoin. New coins first emerged in the 2010s, such as Litecoin (LTC), Ethereum (ETH), Ripple (XRP), and Dogecoin (DOGE), offering new use-cases or technical refinements, from enabling smart contracts to facilitating faster cross-border payments and supporting community-driven digital assets.

Policy and Regulation Issues

The decentralized, fast-evolving, and global nature of cryptocurrencies brings regulatory challenges. While many nations have started to develop policy frameworks for the exchange, taxation, and risk management of cryptocurrencies as a whole, lawmakers and regulators are usually a few steps behind the rapidly developing cryptocurrency industry.

In the US, cryptocurrency has been subject to anti-money laundering (AML) regulations since 2013 under the Financial Crimes Enforcement Network (FinCEN). However, debate continues over which regulatory bodies should oversee these rapidly evolving digital assets. While the CFTC regulates commodities and the SEC securities, cryptocurrencies often blur the lines of oversight.

The European Union has been more proactive in regulating the cryptocurrency industry, developing a rigorous set of guidelines pertaining to the space. In April 2023, the Markets in Crypto Asset Regulation (MiCA) was passed, establishing that all companies looking to trade or issue cryptocurrencies require licensing. Overall, the European Union has been tightening its rules on institutional players and clarifying requirements for consumer protection. Some countries, such as Bolivia, have installed a nationwide ban on the use of cryptocurrencies.

On the other end, countries like El Salvador have integrated cryptocurrency as a legal tender under the premise of encouraging foreign investment and promoting accessibility to the financial system for all citizens.

Glossary

Blockchain: A decentralized public ledger that records transactions across a network of computers, known for its immutability, security, and transparency.

Double-Spending Problem: The ability to reuse the same digital token or asset for multiple online transfers by manipulating a transaction record; a key issue preventing the success of internet-based currency before Bitcoin.

Protocol: A basic set of rules that allows data to be shared between multiple computers; in crypto, the protocol establishes the blockchain system for recording and transferring digital assets on the internet.

For more information, please visit our website finpolicy.georgetown.edu or email cfmp@georgetown.edu