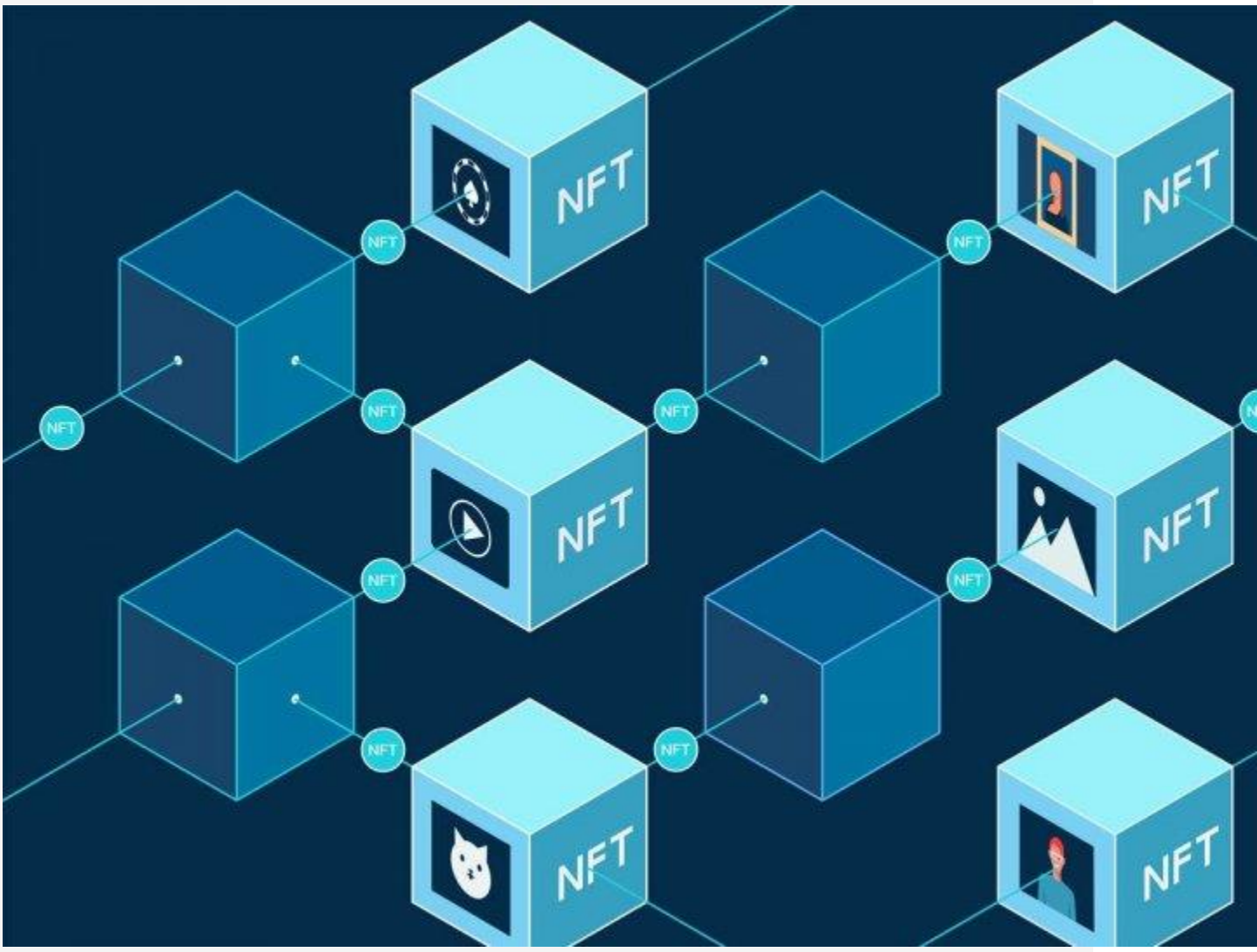
How does blockchain work?



Whether you've studied cryptocurrencies in personal and academic settings, or if you've read an article or two that mention them, chances are you've come across references to blockchain.

While blockchain technologies are customarily discussed in relation to cryptocurrencies, the exciting applications are beginning to spill into debates and conversations in completely separate industries. These

discussions range from data tracking to national currencies to non-fungible tokens (NFTs), and all raise the question: what is blockchain capable of?

It turns out, a great deal. Blockchain technologies are already around us, whether you're aware of them or not. But what exactly makes blockchain technologies so noteworthy? As leading researchers in the field, Stanford faculty offer many insights on these topics, starting with the course Cryptocurrencies and Blockchain Technologies.

Interested in learning about the elementals of blockchain technologies and their functions? Read on for a crash course in all things blockchain.

Getting into the blockchain

Blockchain, as it's moniker suggests, is blocks of data linked into an un editable, digital chain. This information is stored in an open-source decentralized environment, in which each block's information is confirmable by every participating computer. It's designed to have decentralized management instead of the traditional hierarchical systems we're familiar with. A dispersed structure like the blockchain helps to ensure trust, validity and usability.

Blockchain is a constantly evolving and complicated field that offers an increasingly popular channel for online transactions and varied applications. But how does the blockchain work? Key terms – proof of work versus proof of stake, miners, distributed ledger technology, and many more – pose barriers to comprehension. A system that appears vast and complex can be made more transparent through clear steps with explicit terminology explanations.

Key terms important to blockchain technology

As blockchain is a seemingly endless discussion of complicated terms and phrases, it's worth breaking down the steps of a generalized cryptocurrency transaction and taking a good look at a few of the key terms of the field.

Blocks are the ledgers that are being updated and added to, filled with permanently recorded data. Transactions are added to this database and synced with every node of the blockchain. The *block height* refers to the

number of connected blocks at a certain time, growing with every new block stacked on the previous block.

These blocks operate on a *distributed ledger*, meaning that all information and transactions are shared between parties regardless of geography or status. These ledgers can be *permissioned* or *unpermissioned* depending on who is allowed to view it and if there is restricted access or not to the public or private blockchain

The nature of this decentralized block database system keeps hackers from tampering with or changing information on the blockchain as altering a single piece of code would be immediately recognizable against anyone else's copy. Attempting to double spend, fraudulently duplicating the digital currency or asset, is difficult to do because of the distributed ledger transaction system. In this way, the distributed ledger is an immutable record that is consistent and chronologically organized.

Another security measure is the cryptographic *hash*, or *hash function* for transactions within a block. This code takes the input of data of any length and outputs an alphanumeric string, or *hash value*, that acts as a *digital fingerprint*. It is a one-way system that ensures input data is private, secure, and deterministic – the same input will always produce the exact same hashed output for every block. Different blockchains use their own hash algorithms, but the point is the same: creating a unique function for the digital asset transaction.

For the transacting parties, an additional security measure using digital signatures, which involves public keys and private keys, corresponding to an account or crypto wallet. Each party has a public and private key, with public keys being widely accessible and acting like a known email address for the users, and private keys, or secret keys, acting like passwords solely for the owner's use and access. The two keys are dual parts to produce digital signature of a transaction. Specifically, when a transaction is published on the blockchain, the transaction is signed with the private key and can be later verified with the corresponding public key to make sure that the origin of the transaction is legitimate, and the content is not tampered

When it comes to verifying a blockchain transaction and creating the block, the two most popular forms are called *proof of work* and *proof of stake*. These are the consensus processes that are made by nodes in a particular blockchain network. Remember that cryptocurrencies that operate on the blockchain use different verification systems with their own unique structures.

As the first and is the most common mechanism for proving transactions, proof of work is used by many popular cryptocurrencies, including Bitcoin and Ethereum. Proof of work validates transactions when *miners* complete a mathematical puzzle, thus adding blocks to the chain and mining new coins – think Bitcoin miners. For some digital currencies, miners are responsible for adding more to the market. The process of mining is essentially guesswork that requires enormous computational power — and even more energy consumption. The miner who is the quickest to solve a complex mathematical problem relating to the hashed data will be rewarded with a set amount of cryptocurrency as the block is added to the blockchain.

Proof of stake, on the other hand, has *validators* that "stake" cryptocurrency on a certain transaction for block creation. By staking their assets they are entered into a lottery-style selection process, and, if chosen, the validator will receive payment in the form of the transaction costs. Proof of stake is generally fairer as it requires less amassed computational power, meaning those with more resources don't hold a monopoly on verification — which often happens with proof of work systems. It's a compelling system, so much so that Ethereum is making the shift to a proof of stake in 2022. Without the mining feature of proof of stake systems, though, all of the currency has to be pre-mined instead of the steady mining and production of a coin like Bitcoin.

While the verification process is generally attributed to the trading of the digital currency themselves, *smart contracts* are another example of digital assets stored on the blockchain. These are programs in code that allow for self-executing contracts, removing the need for an arbiter or management, and only completing a block when the terms have been met. Ethereum's system, for example, is set up for this form of digital

asset, opening the blockchain to much more than just trading cryptocurrencies.

Blockchain beginnings

While the idea of solidified blocks of data has been around for a while, blockchain technology as it is currently known is attributed to an individual with the pseudonym Satoshi Nakamoto. In 2008, Satoshi Nakamoto proposed this new concept in a paper entitled "Bitcoin: A Peer-to-Peer Electronic Cash System." A year later the currency was released to the public on the blockchain system as we know it.

The idea that Nakamoto proposed aimed to create a payment system based on public ledger and communal verification, where each computer, or node, in the network would have a copy of all transactions. The now historic early transaction on this novel structure took place several days after the first ever digitally mined coins. Hal Finney became the earliest recipient of crypto through the blockchain, proving that the system worked.

Since this foundation, Bitcoin became very popular and lucrative for many, spurring the creation of altcoins – all digital tokens that followed Bitcoin – that now number over 6,000. But it's not just cryptocurrency transactions that have been getting people excited about blockchain data storage.

Significance of blockchain technology

Bitcoin's system allows users to transfer digital assets in the form of coins without a traditional regulatory or administrative body. Previous digital currencies were prone to counterfeit and fraud, as there was no central fixture to oversee the production of the asset. Thus, blockchain has enabled the first ever formation of digital money.

The significance of Bitcoin's transaction, and one of the reasons the technology is enticing to individuals and private industry alike, is that blockchain structures allow for secure, verifiable, and traceable transactions without centralization. By its very nature, the decentralized blockchain relies on each node connected to the network, and on verifiers to ensure each transaction is accurate and trustworthy. Blockchain protects user information, data transferal, and is near

impossible to hack or manipulate for personal gain. It is a method that, while by no means perfect, changes the traditional path of digital transactions.

This is truly just the beginning of what blockchain technology is capable of, in the market and in direct transfers.

Popular uses for blockchain technology and handling data

Blockchain use cases are growing as industries recognize the potential applications of blockchain technologies in different systems, from tracking data, information and asset transactions to privacy. The strides blockchain tech has made in digital currencies are enormous, enabling the realization of a previously unimaginable concept.

Cryptocurrency popularity

From Bitcoin to Ethereum (ether) to the thousands of other digital currencies currently on the market, cryptocurrencies continue to be the most popular use for blockchain technology and data management – but there are rapidly developing industries that may already be impacted by the trajectory of these technologies.

The growing number and value of these currencies signals the importance of blockchain technologies, systems that have allowed digital currencies to become commonplace. The veritable gold rush towards this futuristic trading technology continues to ebb and flow with market predictions and attitudes thanks to the blockchain system.

It's not just individual investors who are excited about crypto. From smart contract functions to the adoption of crypto currencies as legal tender – Sri Lanka adopting Bitcoin as discussed in free Stanford Online webinar, "The Future of Blockchain and Cryptocurrencies," for example – signals the long term effects of blockchain technology.

Extended popularity of blockchain technology

A decentralized ledger that everyone can check to ensure trustworthiness and protects user data goes far beyond financial transactions. The potential for blockchain applications are endless, from supply chain tracking to workflow automation.

Regardless of the future of each individual cryptocurrency, many companies are already implementing blockchain technology for their own purposes. For some, blockchain solutions look like supply-chain tracking that gives all customers insight into the reliable sources of their product. For others, it's about proof of authenticity, streamlining documentation, or simply increasing customer transparency and accessibility.

Anthem, for example, is an Indianapolis health insurance company currently using a blockchain data tracking system that gives customers access to their own data which promotes oversight and greater clarity for customers. Or consider Dole Foods that is attempting to streamline the supply-chain process and transaction data to increase transparency about food quality, enabling the company leaders to track their produce from the farm to the dinner table.

From home equity loans in California, oil production in the Netherlands, or the UN's iris scanning ID process, blockchain technology implementation is expanding globally.