

What is Blockchain and How Does it Work?

The problems that arise with the internet that we have today include the storage of data centrally. Data from the users of the internet are stored centrally on a stand-alone computer. Such data can be sent and retrieved by a client to create personalized, sometimes intrusive ads to users. Centralized data structures raise issues of privacy, security, and control. Blockchain, its structures, and network have provided solutions to these problems. How? You may ask. Follow me.

Blockchain networks reinvent the way data is stored and managed over the internet by providing a unique set of data collectively managed by nodes (any system or device connected to a network) in the network. Blockchain technology is the driving force of the next-generation internet, the Web3.

What is Blockchain?

A blockchain is a digital ledger of transactions maintained by a network of computers. Blockchain technology eliminates third parties in web transactions. A common use case would be that of a traditional bank transaction. Let's say, for example, you want to send money to a stock broker you met online. The stock broker is three thousand miles away from you. For the transaction to happen, you would need your bank and his bank to act as trusted intermediaries for that transaction to be complete. With blockchain technology, however, you can have Peer-to-peer transactions without these intermediaries. Each transaction made on the network is approved by the nodes on the network and recorded in batches of data called 'blocks'.

Blockchain technology allows the security of records of transactions as each transaction is recorded on a block with each block chained together in a series of blocks. The growing list of chained blocks is also referred to as a ledger. A manipulation attempt would cause the hash value of the manipulated ledger to differ from the hash value on the copies of the ledger on all other nodes. Every independent node on each blockchain network has the latest version of the ledger, which contains transactions that have been made and can also verify transactions.

The use of blockchain technology has become popular over time with the growth of cryptocurrencies, and tokens - fungible and non-fungible. It also promises use in other scenarios such as having a legal contract or used in other industries such as banking, health care, insurance, and any other industry that might need to authorize or record a series of transactions and actions.

How then does Blockchain Work?

The concept of Blockchain or "chain-of-blocks" was introduced by the Bitcoin white paper in October 2008. Although the idea of a decentralized web has been in theory way before then, only Bitcoin and the blockchain technology it is built on have been able to bring this concept to life. The paper, published under the pseudonym, Satoshi Nakamoto presented a system

where each computer in the network maintains a duplicate copy of a ledger of transactions, serving as the network's central point of reference. This ledger, which is updated and managed by all network nodes, serves as a common data set that all actors may rely on, even if they might not know or trust one another. With the introduction of this technology, it is no longer necessary for trustworthy third parties to mediate interactions between parties who do not know or trust one another, reside in different countries, are subject to different laws, or have non-binding contracts.

Instead of a bank approving financial transactions, in the Bitcoin network, all computers in the network review their copies of the ledger for the transaction's validity and then unanimously affirm transactions by majority consensus. No one is more trustworthy than another user. A P2P network of computers running the blockchain protocol confirms transactions by consensus rather than a single reputable third party validating them through their servers with authority (single vote) (majority vote).

Blockchain networks enable distributed control, in contrast to distributed databases, which share data but are maintained and controlled by a single body. Information is shared between organizations and groups of people that do not trust one another without the need for a central administrator.

Behind every blockchain protocol

- The use of public-key cryptography and cryptographic hash functions allows for transparency, security, and privacy.
- Nodes of the P2P Network validate transactions by consensus, following economic incentive mechanisms(Proof-of-Work, Proof-of-Stake.etc.)
- Every node of the network is a client well as a server holding identical copies of the application state (the ledger).

In summary, this is how blockchain works;

P2P Network

A chain of blocks representing the entire transaction history (the ledger) is maintained by each full node in the network.

Game Theory

Each new block of a transaction is added to the blockchain network by consensus or network nodes at even time Intervals. Nodes are rewarded with the native token for validating transactions according to the rules, with a fault-tolerant and attack-resistant mechanism

Cryptography

The network stores all the data in blocks, which are units of encrypted data. The Genesis Block is the first block. Each block has a finite amount of storage. Blocks are "chained" together by cryptography because they record the hash value of the preceding blocks.

Conclusion

There are thousands of other cryptocurrencies that are based on blockchain technology, even if the Bitcoin system is its most well-known use. While it is yet unclear if bitcoin will be able to replace other types of conventional payment systems, blockchain technology applications are expanding quickly, and supporters claim they might bring about significant changes in a variety of industries.

There are practically unlimited possibilities for blockchain in almost every business. The ledger technology can also be used to more effectively track intellectual property in business and music rights for artists. It can be used to detect financial fraud, securely exchange patient medical records between healthcare professionals, and even track patient medical records.

Unarguably, blockchain is reinventing the entire internet. From a decentralized web to cryptocurrencies and tokens. There are numerous use cases for cryptocurrency and in the coming years, blockchain technology will be used more in industries across the world