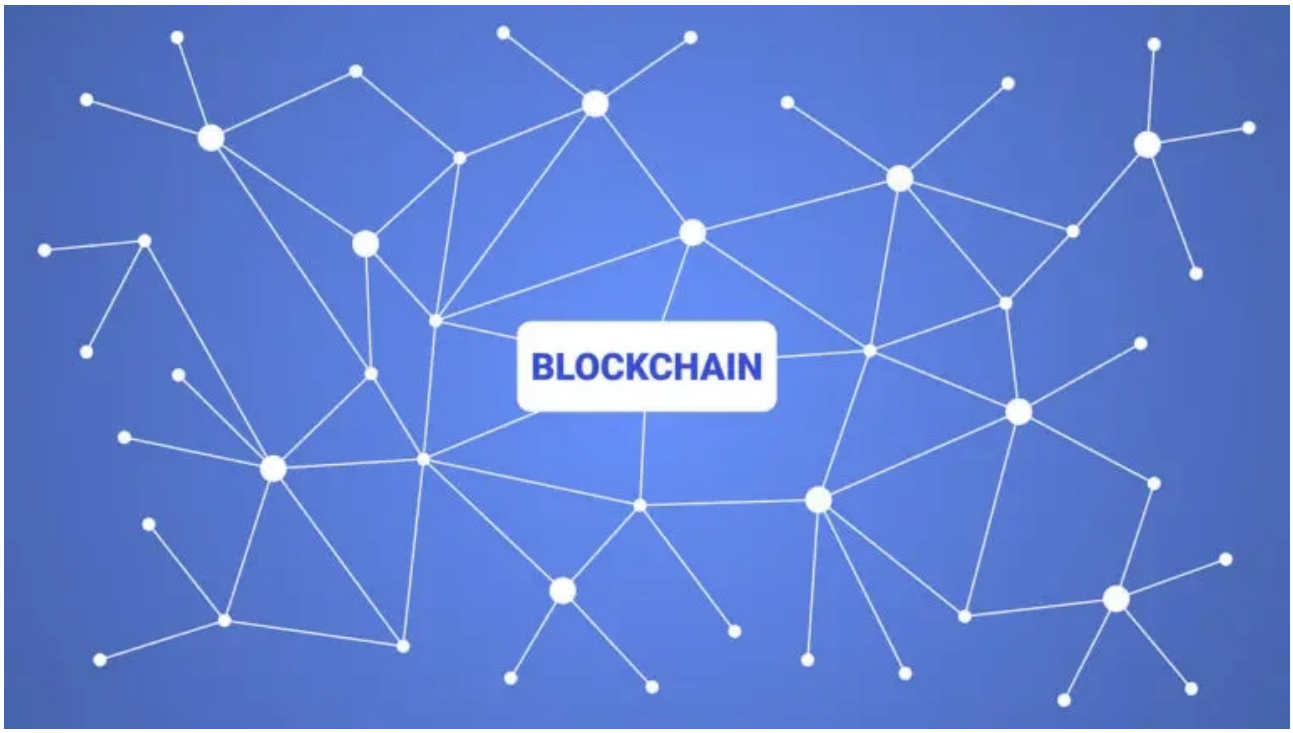
Blockchain

Introduction



The Blockchain is a growing collection of records known as blocks that are linked together using cryptography. Each block includes a cryptographic hash of the previous block, as well as a timestamp and transaction data (generally represented as a Merkle tree).

The timestamp demonstrates that the transaction data existed at the time the block was published in order to be included in its hash and forms the backbone of Cryptocurrency technologies.

Because each block contains information about the one before it, they form a chain, with each new block reinforcing the ones before it. As a result, blockchains are resistant to data modification because, once recorded, the data in any given block cannot be changed retroactively without affecting all subsequent blocks.

Blockchains are typically managed by a peer-to-peer network for use as a publicly distributed ledger, with nodes adhering to a protocol in order to communicate and validate new blocks.

Although blockchain records are not unalterable due to the possibility of forks, blockchains can be considered secure by design and represent a distributed computing system with high Byzantine fault tolerance.

In 2008, a person (or group of people) going by the name Satoshi Nakamoto created the blockchain to serve as the public transaction ledger for the cryptocurrency bitcoin. Satoshi Nakamoto's identity is still unknown to this day and remains a mystery.

With the introduction of bitcoin's blockchain, it became the first electronic money system to address the double-spending problem without the assistance of a trusted authority or central server.

The bitcoin design has influenced the development of additional publicly accessible applications and blockchains that are commonly used by cryptocurrencies such as Etherium and numerous others.

The blockchain is regarded as a type of payment rail. Private blockchains have been proposed for commercial use, but Computerworld dubbed the marketing of such privatized blockchains without a proper security model "snake oil."

Others, however, have argued that permissioned blockchains, if carefully designed, may be more decentralized and thus more secure in practice compared to permissionless ones.

Blockchain technology can be used in a wide range of areas outside Cryptocurrency and payments by software developers in areas such as smart contracts, decentralized file storage and digital identity authentication.

Background history

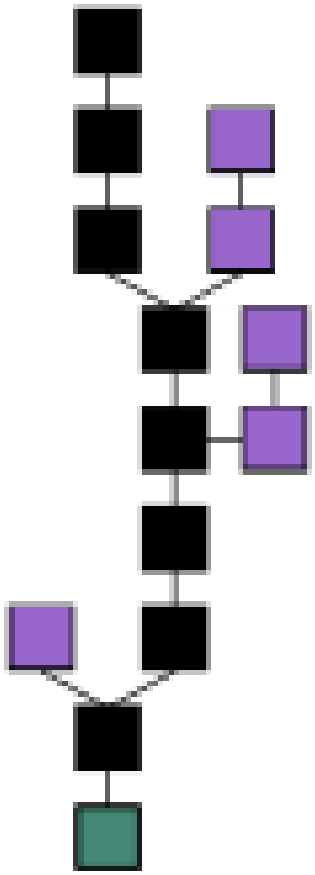
Stuart Haber and W. Scott Stornetta described a cryptographically secure chain of blocks in 1991. Satoshi Nakamoto implemented the design as a key component of the cryptocurrency bitcoin in 2008. By 2016, the term "blockchain" had become popular as a single word.

The bitcoin blockchain file size reached 20 GB in August 2014. (gigabytes) In January 2015, the size had nearly tripled to nearly 30 GB, and between January 2016 and January 2017, the Bitcoin blockchain grew from approximately 50 GB to 100 GB.

The ledger size had exceeded 200GB by early 2020. In May 2018, Gartner found that only 1% of CIO's indicated any kind of blockchain adoption within their organizations. Based on this data only 8% of CIO's were in the short-term planning phase with blockchain technology in May 2018.

According to Accenture, blockchains achieved a 13.5 percent adoption rate in financial services in 2016, putting them in the early adopters category.

Technical structure



A blockchain is a decentralized, distributed, and frequently public digital ledger comprised of records known as blocks. It is used to record transactions across multiple computers so that any involved block cannot be changed in the future. This enables participants to independently verify and audit transactions at a low cost.

The use of a blockchain removes a digital asset's ability to be infinitely reproduced. It verifies that each unit of value was transferred only once, thereby resolving the long-standing issue of double spending.

A blockchain has been described as a protocol for exchanging value. It creates a record that obligates offer and acceptance.

Logically, a blockchain can be seen as consisting of several layers:

- Infrastructure layer (physical hardware been used)
- Networking layer (node discovery, information propagation and verification)
- Consensus layer (provides proof of work & stake)
- Data layer (blocks & transactions)
- Application layer (smart contracts/dApps, are examples of this)

Types of blockchains in existence

The following list are some of the different types of blockchains in existence:

Public blockchains

Access to a public blockchain is completely unrestricted. Anyone with an Internet connection can send transactions and serve as a validator for it (i.e., participate in the execution of a consensus protocol). Typically, such networks provide monetary rewards to individuals that protect them and use a Proof of Stake or Proof of Work methodology.

Examples of public approaches include Bitcoin and Etherium.

Private blockchains

A private blockchain is only accessible to members who have been granted access or those who have been invited by network administrators. Access to participants and validators is restricted.

To differentiate open blockchains from other peer-to-peer decentralized database applications that are not open ad-hoc compute clusters, the term Distributed Ledger (DLT) is typically used for private blockchains.

Hybrid approaches

A hybrid blockchain is one that combines centralized and decentralized features. The chain’s exact operation depends on which parts of centralization and decentralization are used.

Disruption to the traditional financial system

Due to the decentralized nature of the blockchain and Cryptocurrencies traditional banking is expected to be disrupted as the technology gains more momentum.

Whilst traditional banking can be disrupted it can also benefit greatly with the technology. Many banks in recent years have started adopting this technology to improve their own processes and customer experiences.

Ability for individuals and businesses to transfer money overseas or across borders without delay and significantly less feesIncreased transparency and open log of transactions allowing individuals to see information about transactions to verify their legitimacy

Instant lending ability which will provide more accessibility to financial services

Increased freedom and decentralization to trade commercial assets and investments

Strong security and identity measurement to cut down fraud and improve overall transparency

Interoperability between different blockchains

Interoperability in blockchain refers to the ability of two or more software components to collaborate despite differences in language, interface, and execution platform.

The goal is to facilitate asset transfers from one blockchain system to another. A recent working group of the Internet Engineering Task Force (IETF) has already produced a draft of a blockchain interoperability architecture that can be utilized.

Conclusion

We hope you found this resource to be helpful and gained a better understanding of the technology. If so be sure to follow agrtech on our social profiles to keep updated with new content we share.

Originally published here:

https://agrtech.com.au/glossary/blockchain/