BLOCKCHAIN TECHNOLOGY AND REAL-WORLD USE CASES

INTER PROBE
INTELLIGENCE & ANALYTICS

DECEMBER

Monthly Newsletter

BY INTERPROBE'S
CRYPTOGRAPHY DEPARTMENT

Blockchain technology entered our lives in 2008 with the publishing of Satoshi Nakamoto's whitepaper "Bitcoin: A Peer-to-Peer Electronic Cash System". Then, Bitcoin became the first application to leverage blockchain technology by recording the first asset transfer on a public blockchain ledger. Most people thought for a while that Bitcoin and blockchain were the same things; however, blockchain technology is a concept far beyond cryptocurrency and Bitcoin. Blockchain is a distributed, decentralized, immutable, and peer-to-peer ledger, and this ledger is copied across various nodes connected in a network.

It consists of blocks in a chain used to store all the events and transactions. To that point, blockchains can be considered databases. A database is centralized, and an administrator owns and controls the data, and thus has a single point of failure. In contrast, since blockchain is a decentralized and distributed system on multiple nodes, an error occurring in any node in the network does not affect the system’s security. Whereas data can only be read and added to the blockchain, data can be created, read, updated, or deleted in databases. The two are quite different when considering such characteristics.

Blockchain makes the data available to anyone anytime, ensuring that all transactions are transparent. It is developed with a range of different cryptography concepts. Hash functions, public-private key pairs, and digital signatures establish the foundation for the blockchain. A blockchain is made of blocks, and these blocks are appended to each other via a link using hash functions. Although the data in the blocks changes depending on the system used, there are generally a nonce value, a timestamp, all transactions written to that block, and the previous block's hash value. Each new block contains transactions that have not yet been verified by the network. After all transactions are verified, new blocks are created. This verification process is called proof-of-work (PoW), which solves the double-spending problem. In PoW, users who want to create the next block and win the reward are called miners. They compete to find a solution to a cryptographic hard problem in order to have the right to mine a block. When one of them finds it, they add that block to the blockchain and broadcast it to the network. PoW is one of the most well-known consensus mechanisms, first used by Bitcoin. However, the entire bitcoin mining mechanism requires high energy consumption and a longer processing time. Therefore, Ethereum has designed its proof-of-stake consensus mechanism in 2022 because it is more secure, less energy-intensive, and better for implementing new scaling solutions than the previous PoW structure. Nevertheless, Ethereum Classic, Monero, Dash, Zcash, Dogecoin, and other cryptocurrencies continue to use Proof-of-Work.

Cryptographic hash functions and digital signatures have an essential role in the blockchain. Hash functions maintain the integrity of the data stored in each block linking the blocks to one another. Since the slightest change in the block completely changes the hash value, that block becomes invalid and is not included in the chain. Digital signatures ensure that the message received by a recipient has come from the sender claiming to have sent the information. This property is called non-repudiation. In addition, they also assure recipients that messages have not been altered in transit. Blockchain-based systems generally use ECDSA as a digital signature algorithm while using SHA-256 for secure hashing.

A block is approximately mined every 10 minutes. Therefore, transactions need to be verified in an efficient and secure way. Merkle tree is a data structure that compresses data for storing blockchains with a tamper-free component built in. It is based on hashing principles, with each hash becoming a part of the next hash to create a tamper-resistant data storage model, constructed in a bottom-up approach. Merkle trees are created by repeatedly calculating hashing pairs of nodes until only one hash is left. This hash is called the Merkle Root. It enables secure and fast content verification for a user to verify whether a transaction is included in the block.

A blockchain network can be built in a variety of ways. They can be public, private, permissioned, or consortium. A public blockchain is open to anyone to join and participate in basic activities such as reading, writing, and auditing. These immutable and distributed networks are ideal for participants who do not trust one another but still want to interact in a network and participate in consensus. Immutability, distributed ledger, and low entry barriers are the benefits of a public blockchain. Furthermore, the large number of network participants who join a secure public blockchain protects it from data breaches, hacking attempts, and other cybersecurity issues. Bitcoin and Ethereum are examples of public blockchains.

Participants in a private blockchain can only join the network if they receive an invitation or if their identity or required information is authentic and verified. Only one organization governs the network, deciding who can participate, implementing a consensus protocol, and maintaining the shared ledger. Activities like who can write to the ledger and what transactions they can participate in are restricted. The operator can only override, edit, or delete necessary entries on the blockchain. This increases trust and confidence between participants depending on the use case. Private blockchains focus on promoting transparency by not protecting user identities much. These are valuable features for supply, finance, logistics, and other business areas. Other advantages of a private blockchain are that it has compliance support and uses efficient consensus algorithms (such as BFT or POW). Since the nodes are distributed locally and the system has much fewer nodes to participate in, the transaction and, therefore performance are faster. IBM, Hyberledger Fabric, and Multichain are examples of private blockchains.

A permissioned blockchain is a mix of public and private blockchains. Anyone can join the network after verifying their identity and receiving specific permissions, but users can only perform certain actions based on their permissions. EOS and Ripple are examples of permissioned blockchains.

A consortium blockchain is not open to anyone; only pre-selected participants are accepted. These pre-selected participants or organizations control who can submit transactions and access data. If participants show malicious behavior, they are discarded from the network by other participants. Even if they are discarded, this may not be a very effective solution in a public blockchain, because creating new identities and participating in a public blockchain is very easy. That’s why consortium blockchains are generally useful for smaller groups. Corda, and Quorum are examples of consortium blockchains.

Blockchain simplifies the process of recording transactions and tracking assets in a business network. A blockchain network can track and trade virtually anything of value, lowering risk and costs for all parties involved. This technology could lead to faster and cheaper transactions, automated contracts, and increased security for financial service providers, logistics, automotive sectors, etc. Although blockchain technology is still in its early stages of widespread adoption, it is already being used by several sectors and businesses.

FINANCE SECTOR

Blockchain technology has been designed from the beginning of Bitcoin to move assets without needing a central governing body. As blockchain technology has advanced, transactions have become faster and cheaper. Ripple is a well-known example of this, and uses blockchain technology for RippleNet, a decentralized global network of banks and payment providers. Financial institutions using blockchain technology may be able to provide faster money transfers. In this way, international money transfers, which sometimes take hours or even days, are realized within seconds and without paying too many fees.

Contracts are critical in the financial industry, and companies spend considerable time on them. It is possible to shorten this process and make it efficient through smart contracts. A smart contract is a program that runs on a blockchain that can impose contractual agreements. They typically function as digital agreements that enforce a set of rules. These rules are predefined by computer code, which is replicated and executed by all network nodes. An insurance company, for example, could use smart contracts in order to expedite the claims process. When a client submits a claim, it is automatically reviewed by the codes, and if the claim is valid, then the company pays the client.

SUPPLY CHAIN

IoT devices such as smart sensors and RFID tags can efficiently record when specific products move through various stages of the supply chain, and what their condition is (temperature, vibration, humidity, and so on). Thus, companies can easily understand and detect issues fast. It also implies possible cost savings. Most food we eat results from a complex global supply chain that includes a web of production, processing, packaging, storage, and distribution. In addition, people can see when the food that they see in the market or that comes to their table is produced, under what conditions it is transported, and whether it deteriorates while being transported using blockchain technology. Many food safety issues, such as cross-contamination and disease transmission, are hard to track in isolation. Blockchain's authenticity and integrity make it especially well-suited for handling these issues. Since 2017, not only the food industry, but also companies from other industries have been trying to develop solutions to such problems by integrating blockchain into their systems.

HEALTH

With the use of blockchain infrastructure in the health sector, it has been observed that some processes have been accelerated and risks have been minimized. For example, hospitals ask for the address information during patient registration and keep this information on record. When a patient moves from one place to another, he cannot update his old address in the records of all hospitals. Having to provide the same information over and over again in the healthcare space is one of the most tedious things that patients encounter. Therefore, it makes everyone's job easier for patients to update their information in one place and automatically renew this information throughout the system. Also, it is crucial that the medication is authentic and all ingredients are exactly what they are supposed to be. Some medications, such as vaccines, have special transport conditions. For this reason, it is necessary that there should not be many fluctuations in conditions during transportation. Blockchain technology can help support the global healthcare industry's development by saving money and encouraging additional investment in critical resources.

Blockchain technology is a promising field to work on and develop. Even if this is the case, it may not be suitable for every business area. Thus, before integrating blockchain into business, answering some questions and considering system requirements will help in making the right decision for the business.

REFERENCES

https://bu lt n.com/blockcha n/blockcha n- n-supply-cha n
https://www. bm.com/top cs/what- s-blockcha n https://med um.com/swlh/a-s mple-gu de-to-understand ng-blockcha n-8dd09356b153
https://www.fool.com/ nvest ng/stock-market/market-sectors/f nanc als/blockcha n-stocks/blockcha n- n-f nance/
https://www.mongodb.com/databases/blockcha n-database
https://ethereum.org/en/developers/docs/consensus-mechan sms/pos/