Blockchain

Blockchain is a type of distributed ledger for maintaining a permanent and tamper-proof record of transactional data. A blockchain functions as a decentralized database that is managed by computers belonging to a peer-to-peer (P2P) network. Each of the computers in the distributed network maintains a copy of the ledger to prevent a single point of failure (SPOF) and all copies are updated and validated simultaneously.

In the past, blockchains were commonly associated with digital currencies, and Bitcoin in particular. Today, blockchain applications are being explored in many industries as a secure and cost-effective way to create and manage a distributed database and maintain records for digital transactions of all types.

How blockchain works

A blockchain ledger consists of two types of records: individual transactions and blocks. The first block consists of a header and data that pertains to transactions taking place within a set time period. The block's timestamp is used to help create an alphanumeric string called a hash.

After the first block has been created, each subsequent block in the ledger uses the previous block's hash to calculate its own hash. Before a new block can be added to the chain, its authenticity must be verified by a computational process called validation or consensus. At this point of the blockchain process, a majority of nodes in the network must agree the new block's hash has been calculated correctly. Consensus ensures that all copies of the distributed ledger share the same state.

Once a block has been added, it can be referenced in subsequent blocks, but it cannot be changed. If someone attempts to swap out a block, the hashes for previous and subsequent blocks will also change and disrupt the ledger's shared state. When consensus is no longer possible, other computers in the network are aware that a problem has occurred and no new blocks will be added to the chain until the problem is solved. Typically, the block causing the error will be discarded and the consensus process will be repeated.

Blockchain platforms

Blockchain platforms can be either permission-less or permissioned. In a public, permissionless blockchain like Bitcoin, every node in the network can conduct transactions and participate in the consensus process. In a private, permissioned chain like Multichain, every node might be able to conduct transactions, but participation in the consensus process is restricted to a limited number of approved nodes.

Blockchain consensus/validation algorithms

Choosing which consensus algorithm to use is perhaps the most important aspect of selecting a blockchain platform. There are four standard methods blockchain and other distributed database platforms use to arrive at consensus. Generally, public platforms choose algorithms like Proof of Work because they require a lot of processing power to compute, but are easy other network nodes to verify.

- Proof-of-work algorithm (PoW)
- Practical byzantine fault tolerance algorithm (PBFT)
- Proof-of-stake algorithm (PoS)
- Delegated proof-of-stake algorithm (DPoS)

Who uses blockchain

Although Bitcoin is currently the most visible use of blockchain, it can be used the same way as any other distributed database. In 2016, the online retail company Overstock.com used blockchain to sell and distributed more than 126,000 company shares, marking the first time a publicly traded company used blockchain to support stock transactions. R3, a global consortium of financial institutions, also uses blockchain to record, manage and synchronize financial information using blockchain APIs for specific platforms.

Today, banks and financial institutions across the globe are exploring how they can use blockchain to improve security. Other industries, including healthcare, government and technology, are investigating how they can use blockchain to enable secure exchange of data such as personal health information, digital assets like downloaded entertainment and real estate deeds. Manufacturing and other similar businesses also see the potential to leverage blockchain to manage smart contracts as well as track materials as they move through their supply chains.

Advantages and disadvantages of blockchain

Experts cite several key benefits to using blockchain. Security is considered one of the major advantages with this technology. It is almost impossible to corrupt a blockchain because information is shared and continually reconciled by thousands, even millions of computers, and blockchain has no single point of failure. If one node goes down, it’s not a problem because all the other nodes have a copy of the ledger.

On the other hand, experts say blockchain also has potential drawbacks, risks and challenges. With public blockchains, there are questions about trust and who is responsible should a problem arise. With private blockchains, there are questions about whether organizations are capable or willing to invest in the infrastructure for IT chargeback, an accounting strategy that would apply the costs of IT services, like database transactions, to the business unit in which they are used.

How Blockchain Works

1 TRANSACTION · 2 BLOCK · 3 VERIFICATION · 4 HASH · 5 EXECUTION

1 Transaction

Two parties, A and B, decide to exchange a unit of value (digital currency or a digital representation of some other asset, such as land title, birth certificate or educational degree) and initiate the transaction.

2 Block

The transaction is packaged with other pending transactions thereby creating a "block." The block is sent to the blockchain system's network of participating computers.

3 Verification

The participating computers (called "miners" in the Bitcoin blockchain) evaluate the transactions and through mathematical calculations determine whether they are valid, based on agreed-upon rules. When "consensus" has been achieved, typically among 51% of participating computers, the transactions are considered verified.

4 Hash

Each verified block of transactions is time-stamped with a cryptographic hash. Each block also contains a reference to the previous block's hash, thus creating a "chain" of records that cannot be falsified except by convincing participating computers that the tampered data in one block and in all prior blocks is true. Such a feat is considered impossible.

5 Execution

The unit of value moves from the account of party A to the account of party B.

ILLUSTRATORS: SORBETTO/ISTOCK, VECTORSTOCK

TechTarget