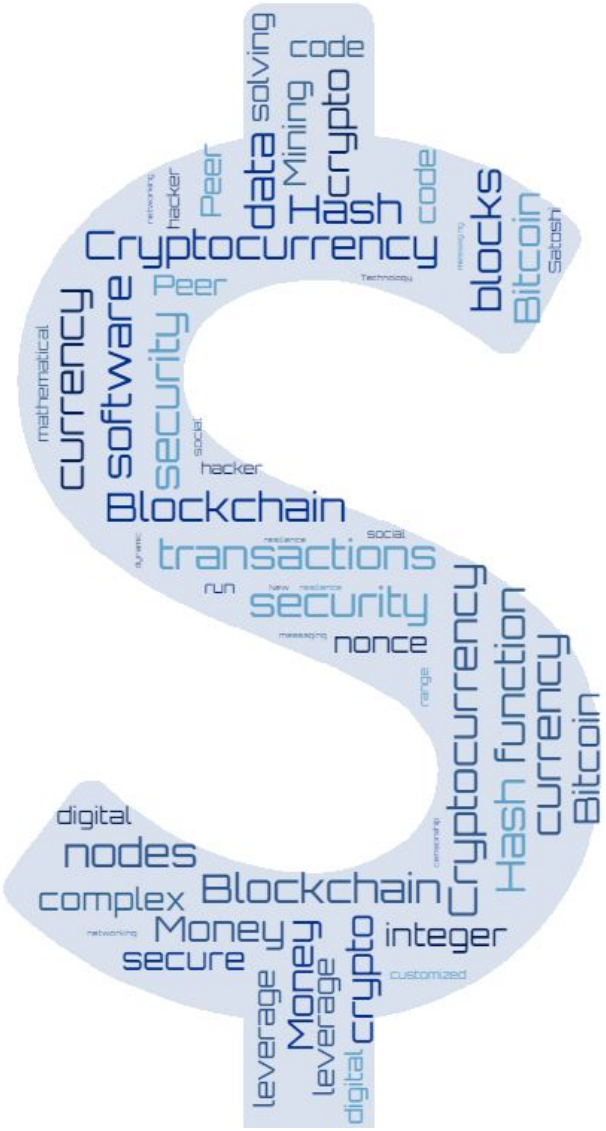
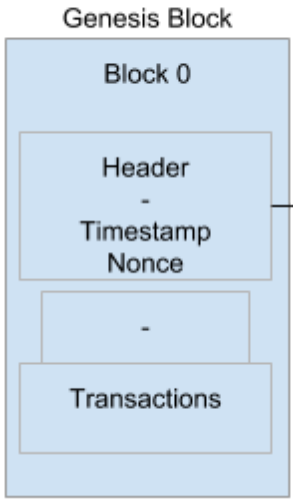
An essential Guide to Blockchain



What is a Block?

A Block is just a record in a system. It could be a simple identification number and a status or a complex list of transactions. Blocks contain certain information which allows them to be uniquely identified from other blocks, and store the information that we want them to.

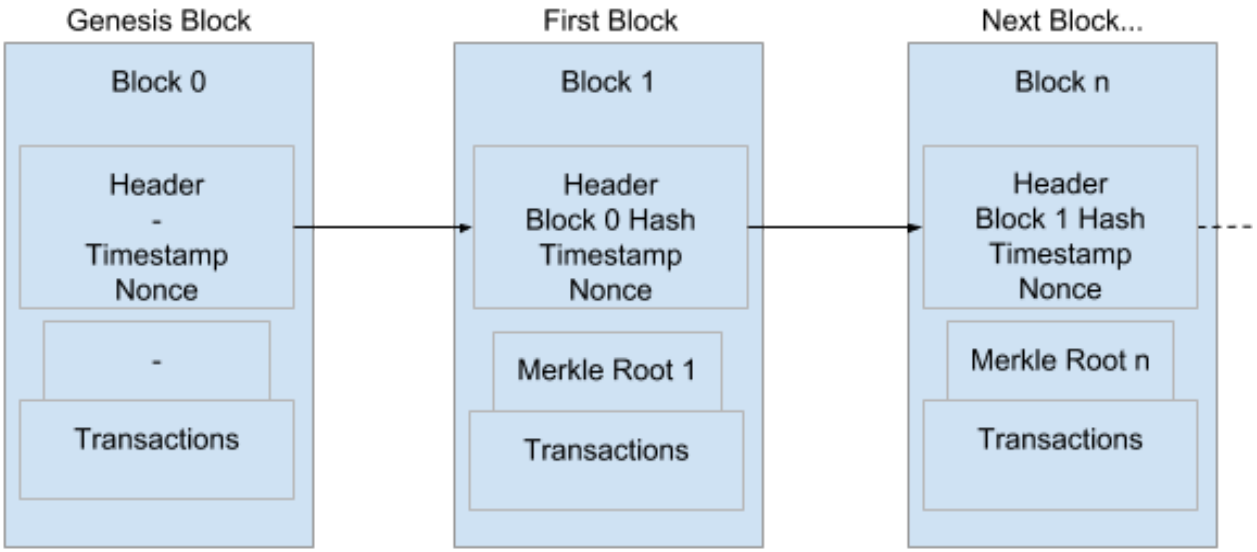


When more than one record exists they are linked together using cryptography. This link is made by using the hash of the previous block. The first Block in the chain cannot contain the hash of a previous block, or a merkle root, this is called the genesis block.

What is a "Blockchain"?

A Blockchain is a continuously growing list of records like a traditional ledger, where records are entered line by line. But unlike the ledgers we are used to, where there is one central copy, the ledger is duplicated and distributed to everyone on the network. Once the records are linked, they become a 'chain'. This chain is permanent and they can never be altered.

The next block always contains the previous block's hash and that joins them permanently together in an unalterable sequence.



What are Nodes?

A node is a powerful computer that runs the cryptocurrency software and keeps the blockchain alive. Running a node is as simple as downloading free software and configuring a normal computer, with enough storage space and processing power. But, Running a node consumes a lot of energy and requires a lot of storage space.

Nodes send information about cryptocurrency transactions across the network to other nodes that it is aware of. A node doesn't need to know all the nodes in the network. Each node is aware of different nodes and so the network grows and the information gets spread across the entire network quickly.

Types of Node

Some of the nodes just spread the information across the network and others additionally perform the task of Mining.

The mining nodes group outstanding transactions into blocks and adding them to the blockchain. To validate the transactions they must solve a complex mathematical puzzle to find a number that is the result of combining the data in the block and passing it through what is called a hash function.

This produces an integer (number) which is called a nonce.

What is a hash function?

The hash function disguises the number in such a way that it is impossible to predict the output. The mining nodes have to guess the number. It is impossible to know which number will work. Two consecutive integers produce very different results and there may be more than one nonce that produces the result, or there may be none. They more attempts a miner makes, the more likely they are to guess the answer, so more power generally means more chance of success. But the element of randomness means that some smaller miners can 'get lucky'.

The more miners that join the network, the more complicated the hash becomes, which is an intentional way designed to balance the number of blocks that can be found. On average this is one block every 10 minutes.

When a miner gets successful hash result it is announced to the whole network and the miner gets a financial reward. As there is no point in other miners continuing to try to guess the validate the transaction and start work on the next block.

Security

If a hacker tried to maliciously change one of the blocks the next block would not contain the correct hash so the chain would break.

Even if someone were successful in maliciously updating all the subsequent blocks, as there is no single copy where the data is stored all the nodes in the network wouldn't be the same. The majority would overrule the node that was changed - as consensus would not be achieved.

The 51% Attack

But there is a well known problem with majority consensus in a blockchain. Only 51% is required to be a majority so if 51% of the nodes were compromised, the information they hold would be considered true and would overrule the remaining 49%. This is called the “51% Attack”.

Why Blockchain?

Blockchain was developed to provide a more open, more secure and cheaper way of completing transactions between 2 entities by offering an alternative to the traditional Trusted 3rd Party method of verification. By relying on consensus to verify transactions and removing the need for a ‘middleman’ many tasks can become cheaper and quicker.

Blockchains can be public or private but this Peer-2-Peer approach provides enhanced security against hacking and fraud which allows easy secure transfers between parties. Through its ‘Open Ledger’ it allows easy auditing for additional security and can be used for a variety of purposes from Proving ownership, verifying communications, transfering money or even tracking items through a supply chain.

Cryptocurrency is just the start, the possibilities for blockchain are endless, be on the lookout for more innovative ways that blockchain is implemented to improve our lives.