

A Blockchain is a constantly growing ledger that keeps a permanent record of all the transactions that have taken place, in a secure, chronological and immutable way.

Ledger -File

Secure - use cryptography , making it permanent lock

Chronological - one after the other transactions

Immutable - cannot be deleted so hence permanent record.



What is BITCOIN

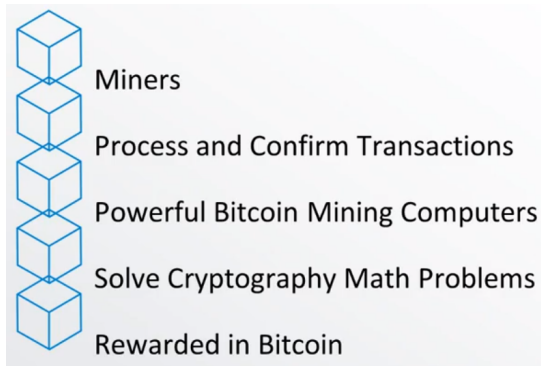
It is a digital asset that can be bought, sold or transferred between the parties.

It holds a value, so you can use these bitcoins as an amount between the organization directly instead of involving 3rd parties just as banks or online transaction websites.

So it's a peer to peer service.

The transfer takes place through block chain which uses global network using thousands of computers creating a decentralized network which is safer compared to centralizing ways such as banks. At each network point of a decentralized network the transaction is checked and verified using maths and cryptography.

Role of Bitcoin Miners



The role of the miner is to build the blockchain of records that form bitcoin ledger. This block contains all the different transactions taken place and this block is added after every 10min to existing created blocks before creating a chain called **Genesis Block**.

Hash Generator - Cryptography.

The data is converted to a hash format for security which is called cryptography in the block chain.

SHA256 Hash

Data:

Hash:

Link - <https://andersbrownworth.com/blockchain/hash>

Note - The data once converted to the hash can not be decrypted i.e immutable.

Blockchain

Block: # 2

Nonce: 35230

Data:

Prev: 000015783b764259d382017d91a36d206d0600e2cbb3567748f46a33fe9297cf

Hash: 000012fa9b916eb9078f8d98a7864e697ae83ed54f5146bd84452cdfd043c19

Mine

Block: # 3

Nonce: 12937

Data:

Prev: 000012fa9b916eb9078f8d98a7864e697ae83ed54f5146bd84452cdfd043c19

Hash: 0000b9015ce2a08b6121f

Mine

Creating a block chain using hash

Each block is created using a unique combination of block , nonce and hash so that the right information i.e data gets attached to a right chain of blocks.

To cross check the information of the block is valid to the hash generated the starting 4 digits of the hash will be zero.

Each block chain comes with a unique hash code of the previous block to maintain the chronology.

Any disturbance occurred at any block of the chain the entire further series of block also gets affected. Hence stop in the network as the hash changes and the next block using the same previous remains the series gets breaks.

So the fault gets detected very easily.

And it needed to be corrected within 10min as after every 10min new block gets added.

This makes block chain a very fast operating service which comes with high security.

To bring the right hash **mine** is used which provides a perfect combination of nonce , block and hash for respective data. But this needs to be followed for all the further blocks as the network gets disturb.

The Four Components of Bitcoin

