Technology Explained: Blockchain Technology

***What is a blockchain?***

In simple words, blockchain is a chain of blocks that contains information. It can also be defined as a distributed ledger that is completely open or accessible to everyone without having any central authority to control.

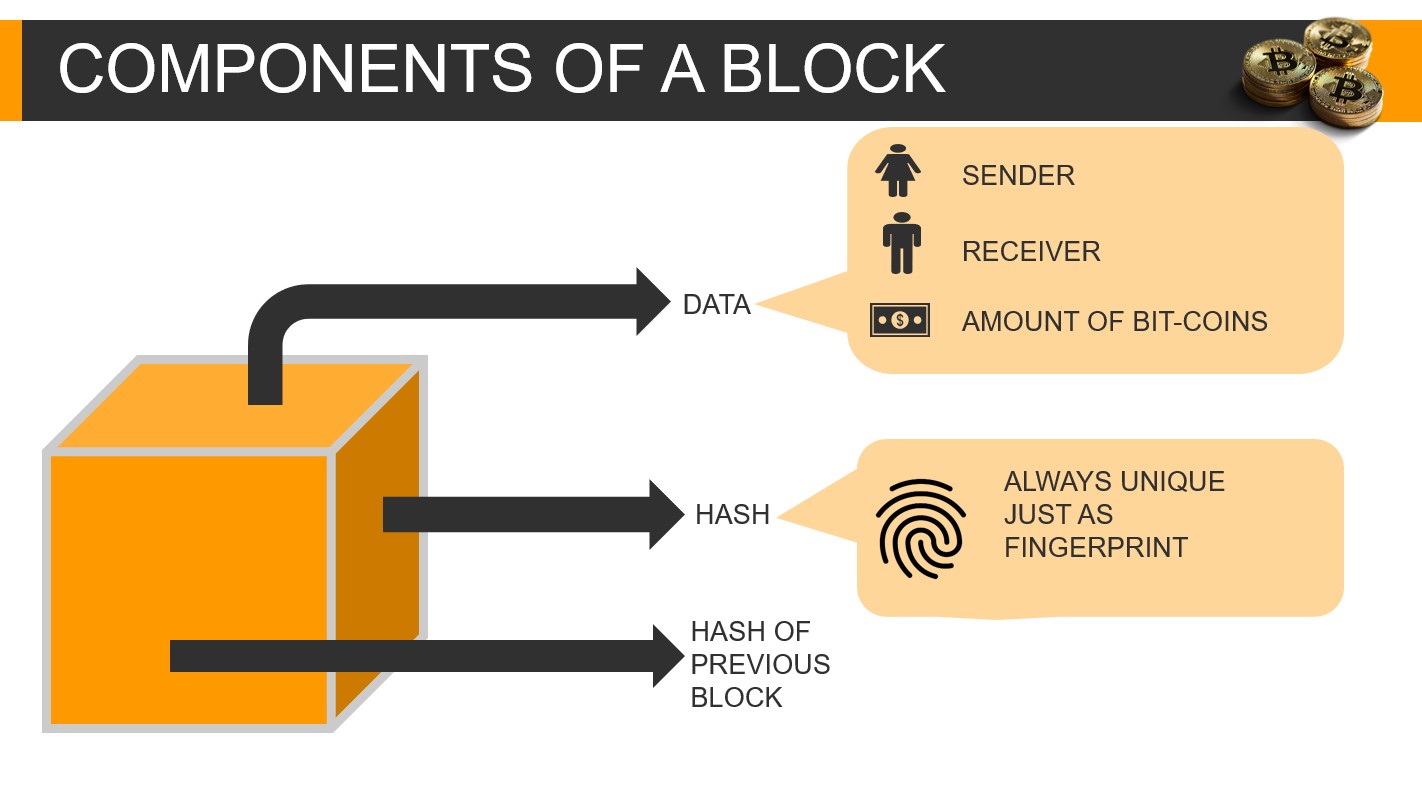
It is an enabling technology for individuals and companies to collaborate with trust and transparency without the interference and dependency of any third party for transaction and sharing of information. Blockchain technology is considered to be the driving force of the next fundamental revolution in information technology. One of the interesting features of this technology is that, once the data is registered in a blockchain it becomes very difficult to change them or tamper them.

***History***

The Blockchain technology was originally introduced in 1991 by *Stuart Haber and Scott Stornetta* and was originally intended to timestamp digital documents so that it’s not possible to backdate or tamper with them.

But this technology was not utilized until it was adopted by *Satoshi Nakamoto* in 2009 to create a digital cryptocurrency bitcoin.

***Components of a block***



Each block contains three main elements like - *Data, Hash, and Hash of the previous block.*

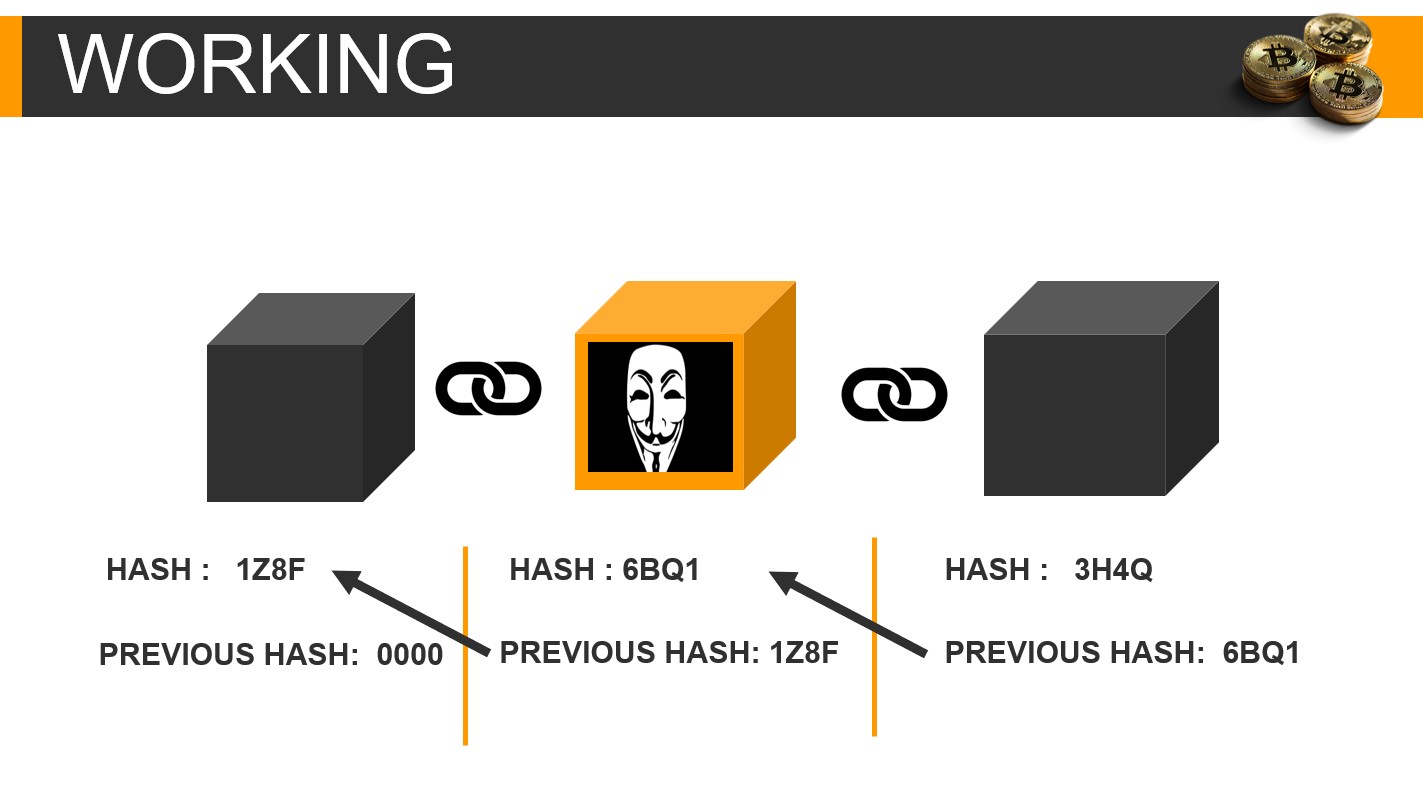
Considering an example of bitcoin blockchain it contains all the information about the transaction such as the information about the Sender, Receiver, and the number of coins.

It also contains the *“Hash”* which can be compared with the fingerprint. It identifies the block and all its content and is always unique just like the fingerprint. Whenever a new block is created its hash is generated immediately.

The third element of the block is *“Hash of the previous block”.*

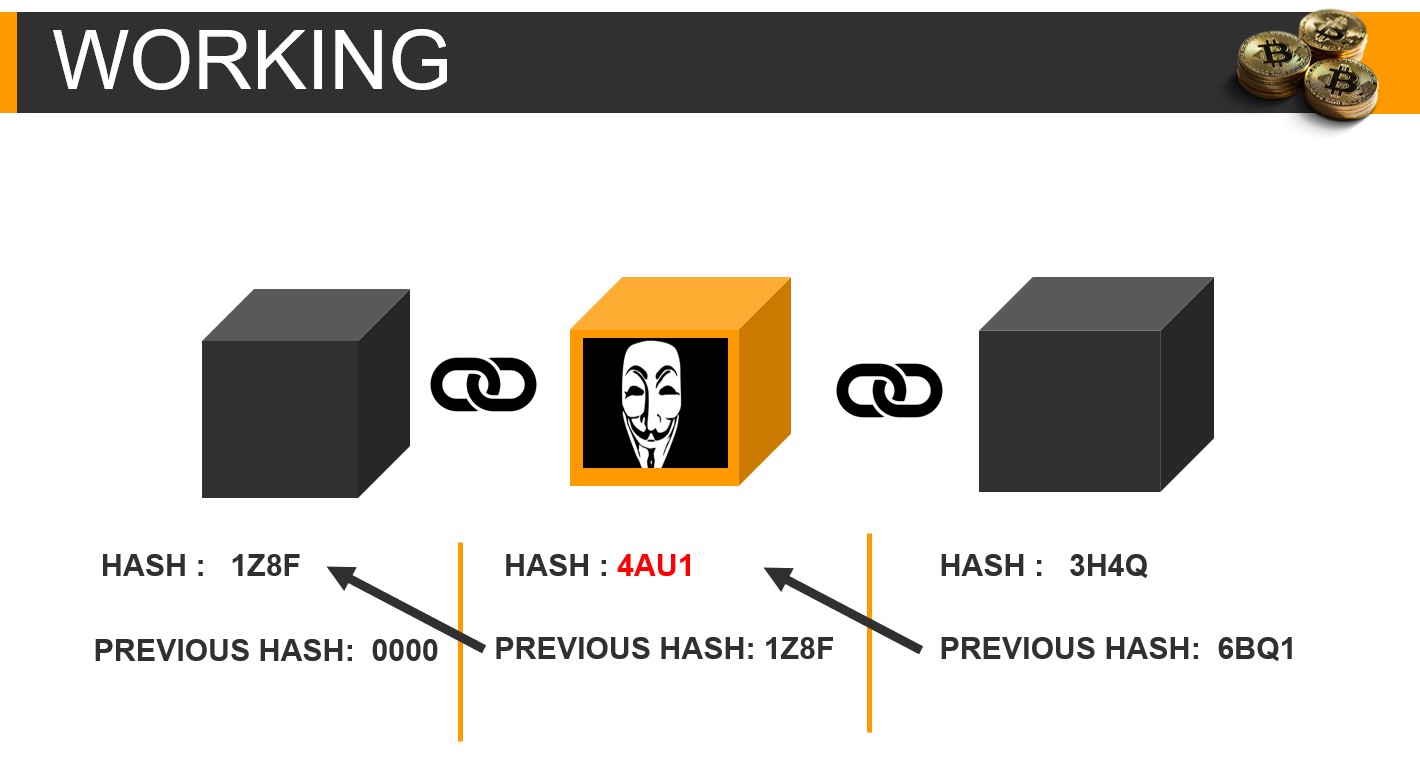
All these elements effectively form a blockchain and it is this technique that makes blockchain technology so secure.

***Working***



Let’s understand the working of the blockchain with an example

Here we have a chain of three blocks, each block has a *hash* and *hash of the previous block*. So, block *number 3* points at block no 2 and *block number 2* point at block number 1. Well, *block number 1* block is the master block so it does not point at any of the blocks and it is called *genesis*.



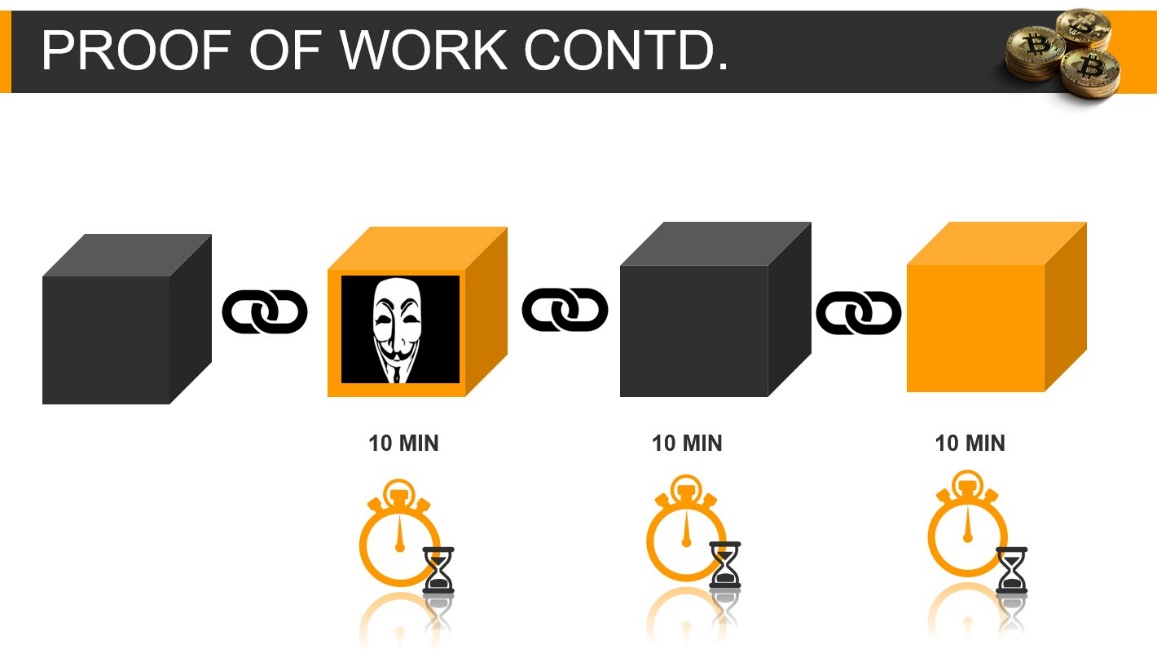
Now if someone tries to tamper with the second block. This causes the change in the hash of the block, which will result in the mismatching of the *hash of block 2* and the *hash of the previous block of block 3.* Thus, making all the following blocks of the blockchain invalid.

So, changing the hash of one block will result in invalidation of all the following blocks in the blockchain.

***Proof of Work***

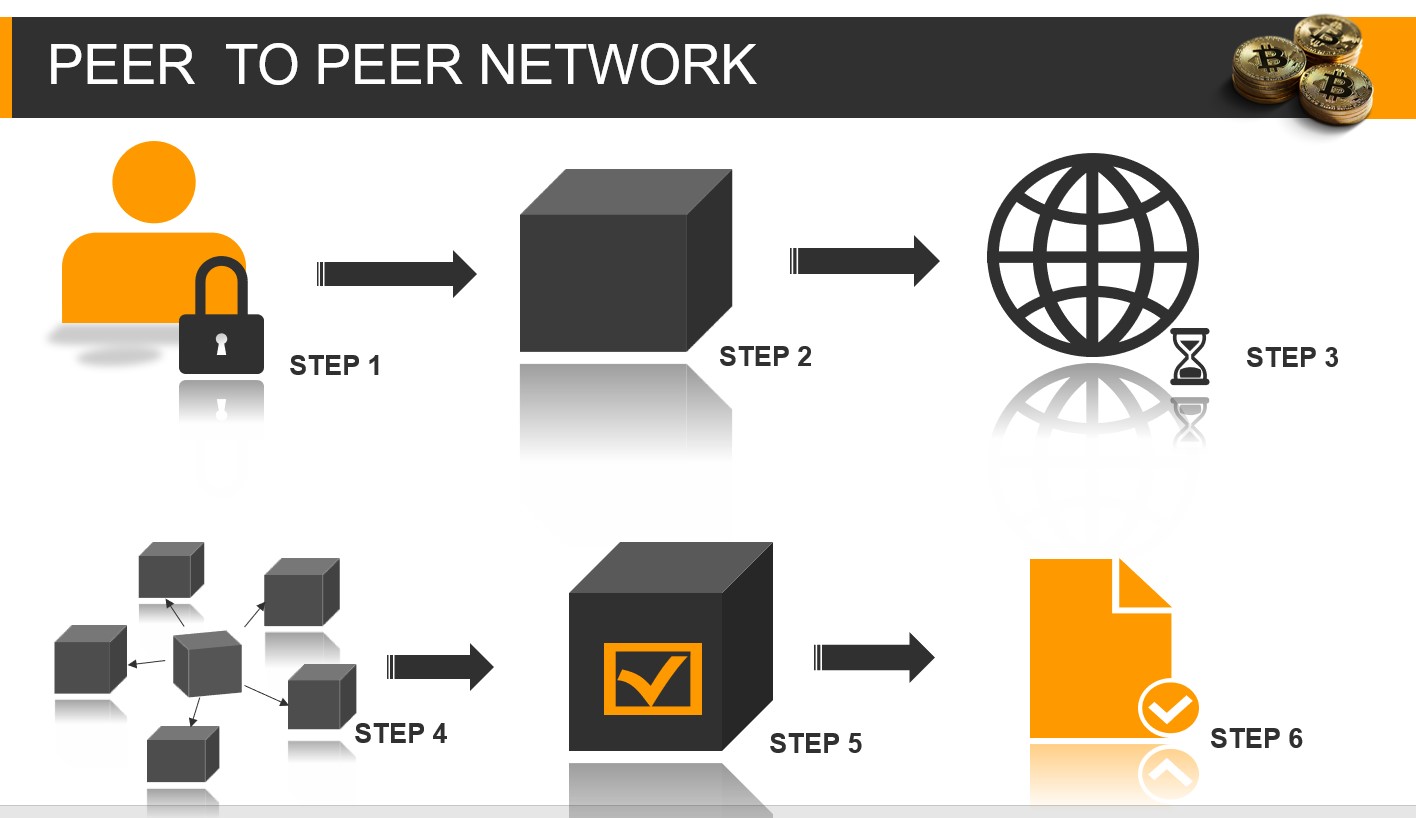
But the use of only *hash* is not enough to prevent tampering of blockchain. Computers these days are very fast and can calculate hundreds of thousands of hashes per second. The changes in all the following block will make the blockchain valid again.

So, to mitigate this, blockchain has something called *proof of work.*



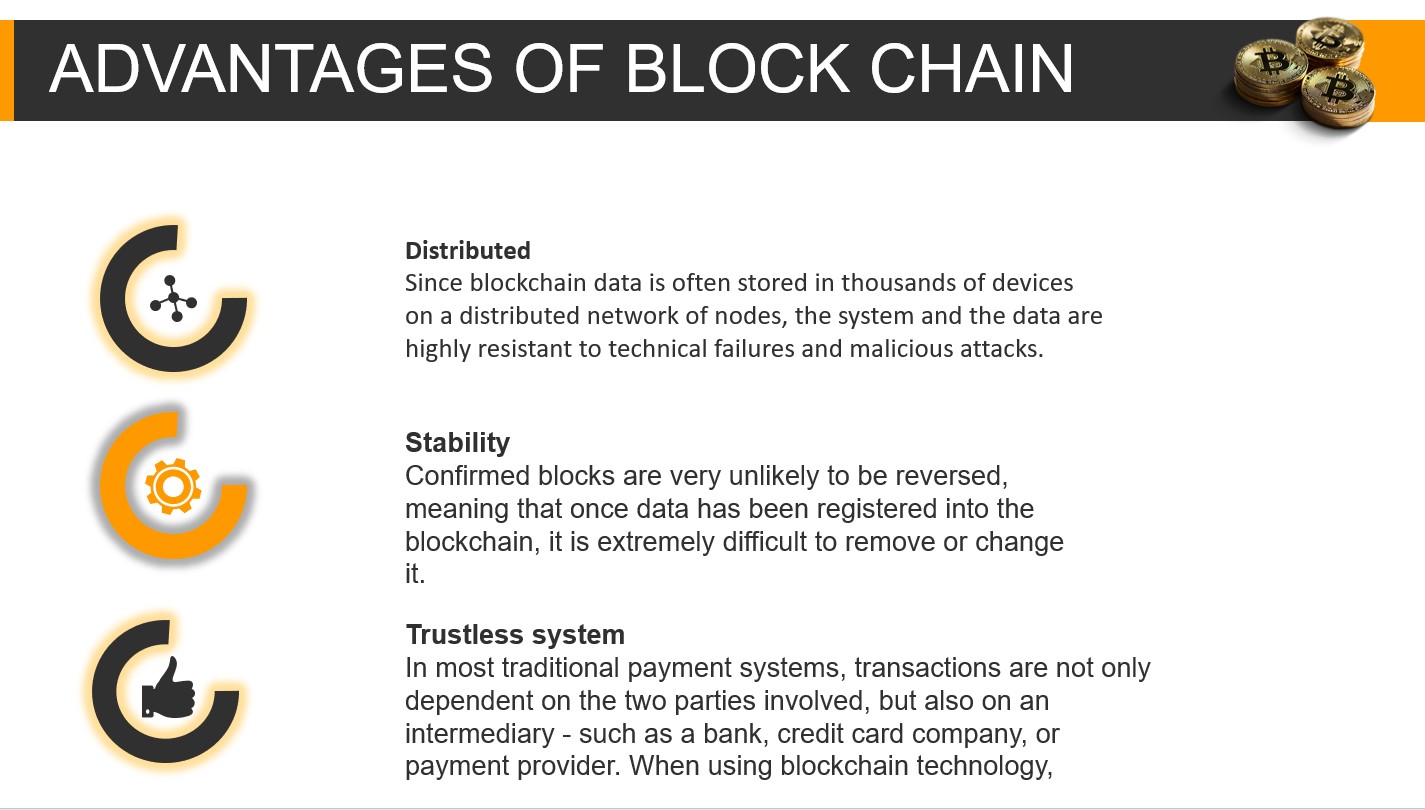
The proof of work slows down the process of the creation of new blocks. In bitcoin case it takes 10 min to calculate the proof of work and if someone changes the hash of one block. It will take another 10 min to change the hash of a single following block and another 10-10min for changing the hash of all the following blocks of the blockchain.

***Peer to Peer network***

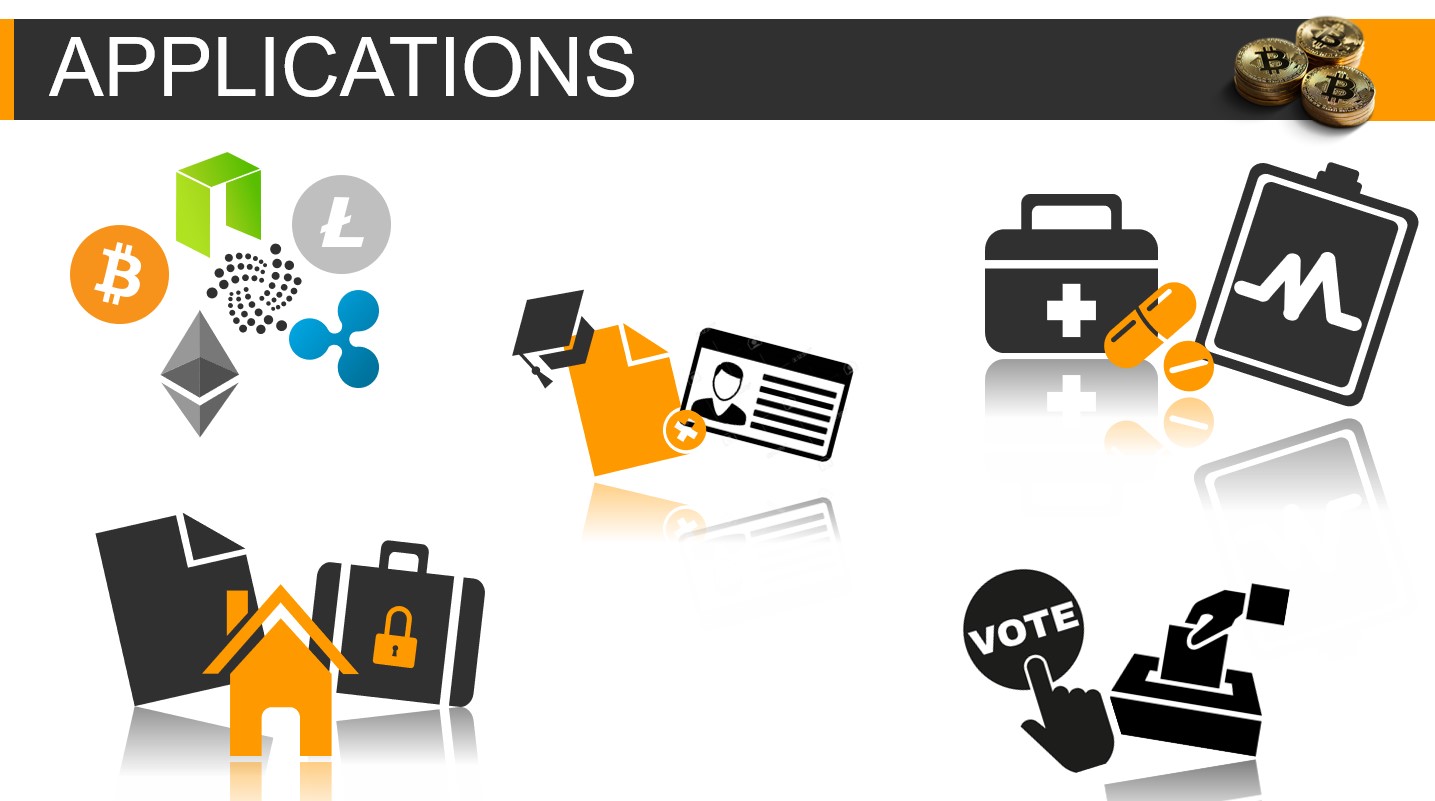


The blockchain technology also comes with another security feature called *peer to peer* *networking*. This means if a new block is created all the nodes or users get a copy of that particular block. Then all the users certify the creation of a new block or transaction. In this way the whole transaction takes place.

***Advantages of blockchain technology***



***Applications of blockchain technology***



This technology is used in cryptocurrencies.

In the medical field for keeping the track of diseases and medical records of the patients.

It prevents the creation of fake ids and educational certificates.

E- notary of properties can be done to reduce disputes.

Fake voting can be prevented with this technology.