UNDERSTANDING A BLOCKCHAIN

A blockchain is a chain of blocks that contains information. This technique was originally described in 1991 by a group of researchers and was originally intended to timestamp digital documents so that it's not possible to backdate them or to tamper with them. However, it was mostly unused until 2009 when Satoshi Nakamoto adopted it to create the digital cryptocurrency Bitcoin.

A blockchain is a distributed ledger that is completely open to anyone. They have an interesting property: once some data has been recorded inside a blockchain, it becomes very difficult to change.

How it works

Each block contains some data, the hash of the block and the hash of the previous block. The data that is stored inside a block depends on the type of blockchain. The Bitcoin blockchain for example stores the details about a transaction such as the sender, receiver and amount of coins.

A block also has a hash. You can compare a hash to a fingerprint. It identifies a block and all its contents and it's always unique, just as a fingerprint. Once a block is created, it's hash is being calculated. Changing something inside the block will cause the hash to change. Hashes are very useful when you want to detect changes to blocks. If the fingerprint of a block changes, it no longer is the same block.

The third element inside each block is the hash of the previous block. This effectively creates a chain of blocks and it's this technique that makes a blockchain secure. The first block is a bit special; it cannot point to previous blocks because it's the first one. It is thus called the "genesis block"