Blockchain

What is Blockchain?

Blockchain is a chain of blocks that contain information. Blockchain was originally intended to timestamp digital documents so that it's not possible to backdat them or to tamper with them. 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 it.

How does a blockchain work?

Each block contain three things:
1.Data
2.hash of the block
3.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 sender, receiver and amount of coins.

A block also has a hash. A hash can compare to a fingerprint. Hash identifies a block and all of its contents and its always unique, just as a fingerprint. Once a block is created, its hash is being calculated. Changing something inside the block will cause the hash to change.So hash is 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 its this technique that makes a blockchain so secure.

For example:
Here we have a chain of three blocks

block1	**block2**	**block3**
hash:1ZFD	**hash:6BQ1**	**hash:3HRT**
pre hash:0000	**pre hash:1ZFD**	**pre hash:6BQ1**

Block3 points to block2 and block2 points to block1. First block is special, it cannot point to previous block because it is first one.so we call first block as genesis block.

What problems do they slove?

Now let's say that you tamper with the second block, this causes the hash of the block change as well. In turn that will make block3 and all following blocks invalid because they no longer store a valid hash of the previous block. So changing a single block will make all following blocks invalid.

But using hashes is not enough to prevent tampering. Computers these days are fast and can calculate hundreds of thousands of hashes per second. you could effectively tamper with a block and recalculate all the hashes of the other blocks to make your blockchain valid again. To mitigate this, blockchains have something called proof-of-work. It's a mechanism that slows down the creation of new blocks.

In bitcoin case it require 10 minutes to calculate proof-of-work and to create a new block to the chain. This mechanism will make difficult to tamper, because if one block is tampered then you will need to recalculate the proof-of-work for all the following blocks.

There is one more way that blochchains secure themselves and that is being distributed.
Instead of using a central entity to manage the chain, blockchains use a peer-to-peer network and anyone is allowed to join. When someone joins this network, he gets the full copy of the blockchain. The node can use this to verify that everything is still in order. When someone creates a new block, that block is send to everyone on the network. Each node then verifies the block to make sure that it hasn't been tampered. If everything checks out, each node adds this block to their own blockchain. All nodes in this network create consensus, they agree about what blocks are valid and which aren't.

So to successfully tamper with a blockchain you'll need to tamper with all blocks on the chain, redo the proof-of-work for each block and take control of more than 50% of the peer-to-peer network.

How they can used?

One of the developments is the creation of smart contracts, these contracts are simple programs that are stored on the blockchain and is used to automatically exchange coins.This technology is used to store medical records, E-notary, taxes.