**Creating a Blockchain**

A blockchain is a continuously growing list of records, called blocks, which are linked and secured using cryptography.

So basically, a blockchain is a data structure like linked lists with a growing set of nodes or blocks.

Most of us would have learned about linked lists in school. Each node has several attributes including id, data, and next node’s address etc.

So, the blockchain is a slightly more complex data structure.

In a blockchain, each node is called a “block” and each block has an index, timestamp, hash of itself, hash of the previous block and of course the data. The data can be anything.

In a cryptocurrency, the data is the details of the transaction like sender’s username, receiver’s username and amount.

Blockchain was initially implemented in 1991 to timestamp digital documents, to make sure they are not backdated or tampered with.

But it didn’t get much attention as timestamping documents is not as cool as bitcoins.

**The concept**

The special thing about the blockchain is that it cannot easily be tampered with.

The hash of each block gives it a unique identity like a fingerprint. And this hash is generated only once when the block is created.

It is generated using the values of all the other attributes of the block. So, if any of the values are changed, the hash will no more be valid and hence the entire block will be invalid. So, this way nobody can tamper with the values stored in the block.

Another thing is if the hash is also recalculated, then it will not be detected as tampering. To avoid this, we store the hash of the previous block. This creates a chain of the blocks and if the hash of any block changes, the chain will be broken and the entire thing will be invalid.

So, to successfully hack a blockchain, the hacker has to know the location of all blocks and simultaneously change all their hashes and relink the whole blockchain. This is not impossible but extremely tedious as there is a mandatory gap of 10 minutes between each transaction. So it beats the whole purpose of life.

**Decentralized Blocks**

These blockchains are not stored in a centralized server. But the blocks are distributed across the internet and they are connected using a peer-to-peer network.

When someone joins the network, they are given the full copy of the network. When they create a new block, the block is sent to all the peers and the validity of the chain is checked. If everything checks out, the block is connected to the chain.