BlockChain WorkShop

- Deependu Jha
- Ankur Ambar Mishra

The Great Recession (2007-2009)

- Lasting from December 2007 to June 2009, this economic downturn was the longest since World War II
- In short, The bad loans and bursting of US housing bubble caused ' The Great Recession'.
- For detailed explanation of the great recession: The Great Recession
- US GDP fell by 4.3%. Inflation and unemployment was at its peak.
- Citizens were angry and frustrated at their government
- Why should they suffer for the mistakes of their government and banks?

Satoshi Nakamoto (Rocky Bhai)

* Rocky Bhai to US citizens

BITCOIN

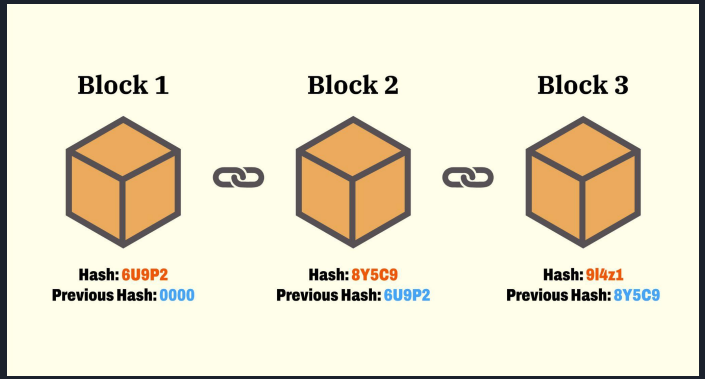
- All these problems happened because of the money that we use (US dollar), and the control that a few people have over all this and they decide the fate of the millions and billions.

~> **So, why not use our own currency and there will be no central authority?**

- **Then who will make sure that, if someone is sending 'X' amount of money to someone else, he/she actually has that much money?**
- **Who will make sure that someone is not faking a transaction?**
- **Who will keep the database of all the transactions, so that we can check that in future?**
- **And, a lot more questions…**

BlockChain (Chain of Blocks)

- A blockchain is a growing list of records, called blocks, which are linked using cryptography.
- Each block contains a cryptographic hash of the previous block, a timestamp, and transaction data.
- When we talk about BlockChains, we inherently mean, it is not centralised, but is an immutable decentralised distributed ledger.



Some Terminologies

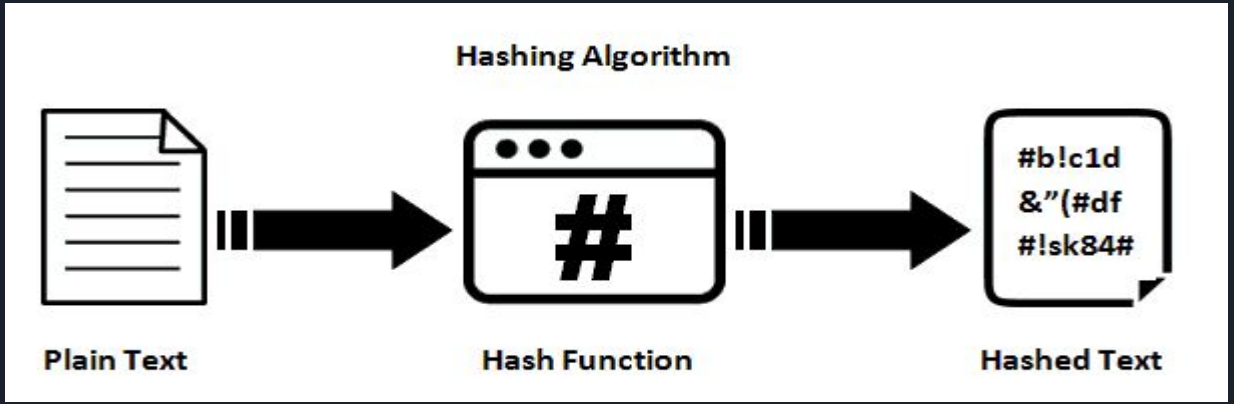
- **Immutable:** Blockchains don't support 'UD' of CRUD operations. They are read and append only. You can't modify a data, neither delete it.
- **Decentralised:** Power is not in the hands of only a few. Decisions are taken by the members of the BlockChain network.
- **Distributed:** BlockChain networks are present around the world and not limited to a particular location. So, the downtime is almost certainly null.
- **Ledger:** A database of all the transactions and data exchanges.

Hence, **BlockChains are essentially 'an immutable decentralised distributed ledger'.**

Some more Terminologies

Hashing:

- A hash is a mathematical function that converts an input of arbitrary length into an encrypted output of a fixed length.
- Thus regardless of the original amount of data or file size involved, its unique hash will always be the same size.
- Moreover, hashes cannot be used to "reverse-engineer" the input from the hashed output, since hash functions are "one-way" (like a fruit juicer; you can't get the apple from apple juice).
- Still, if you use such a function on the same data, its hash will be identical, so you can validate that the data is the same (i.e., unaltered) if you already know its hash.

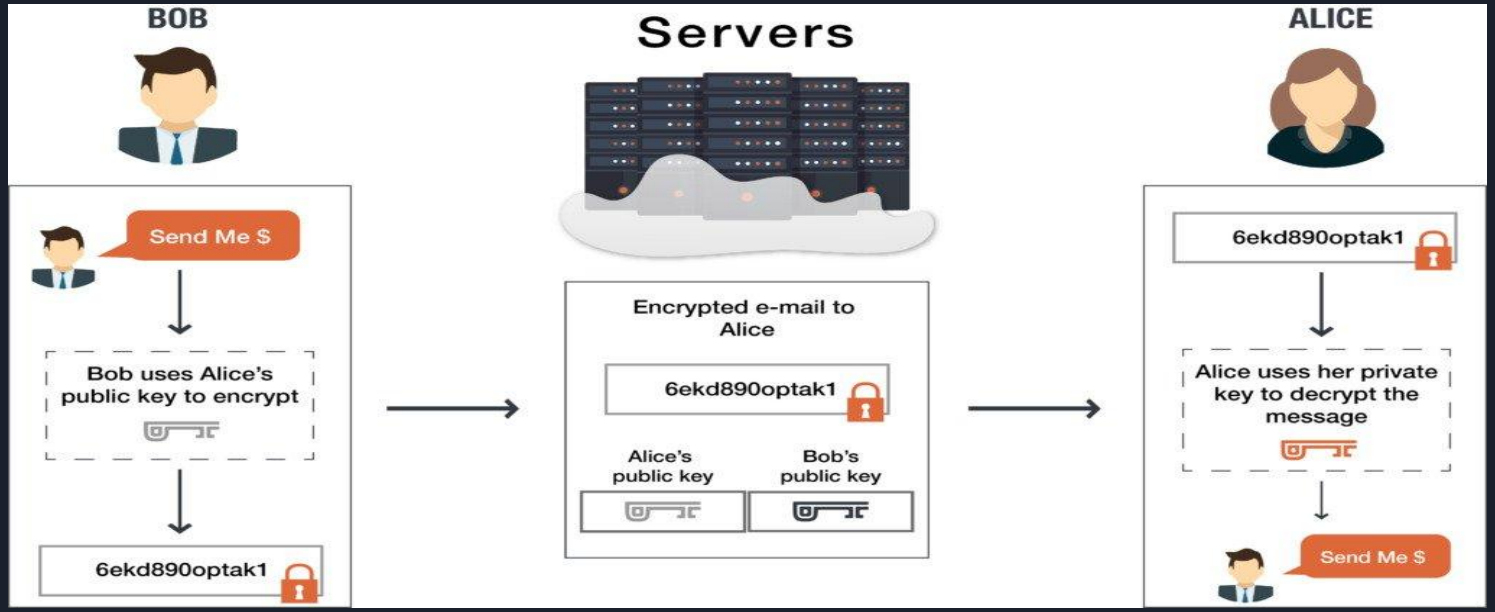


There are many hashing algorithms, but most of the blockchains use: **SHA256 algorithm** (secure hash algorithm-256). **MD5** and **KECCAK** are some other famous hashing algorithms.

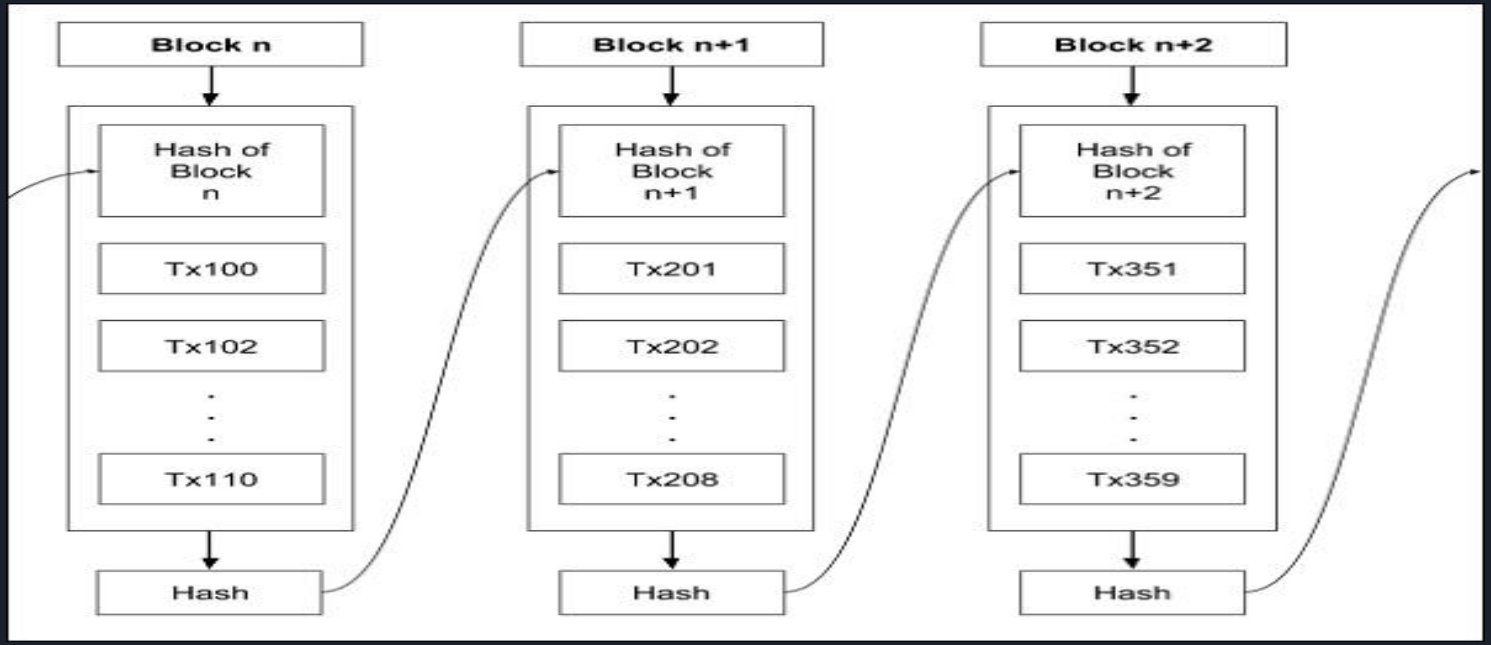
Play with it: https://emn178.github.io/online-tools/sha256.html

Some more Terminologies

Public Key Cryptography (Asymmetric Cryptography):

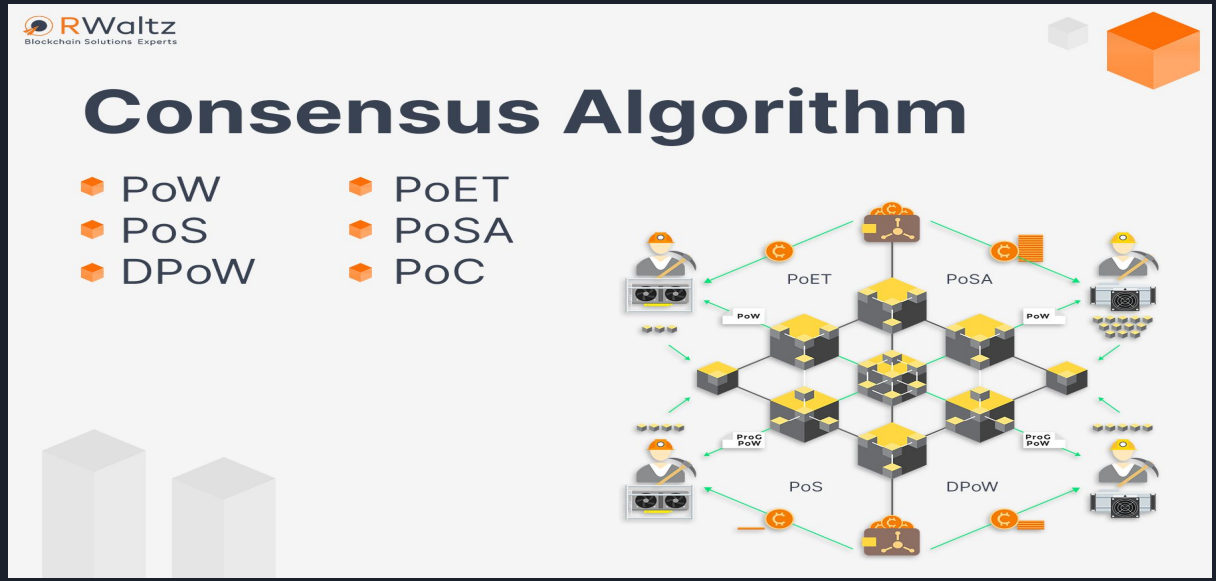


Chaining Of Blocks



Consensus Algorithms

Since there's not a central authority, but multiple individuals. **How will we come to agreement when there's conflict about the transactions and data?**



Proof of Work

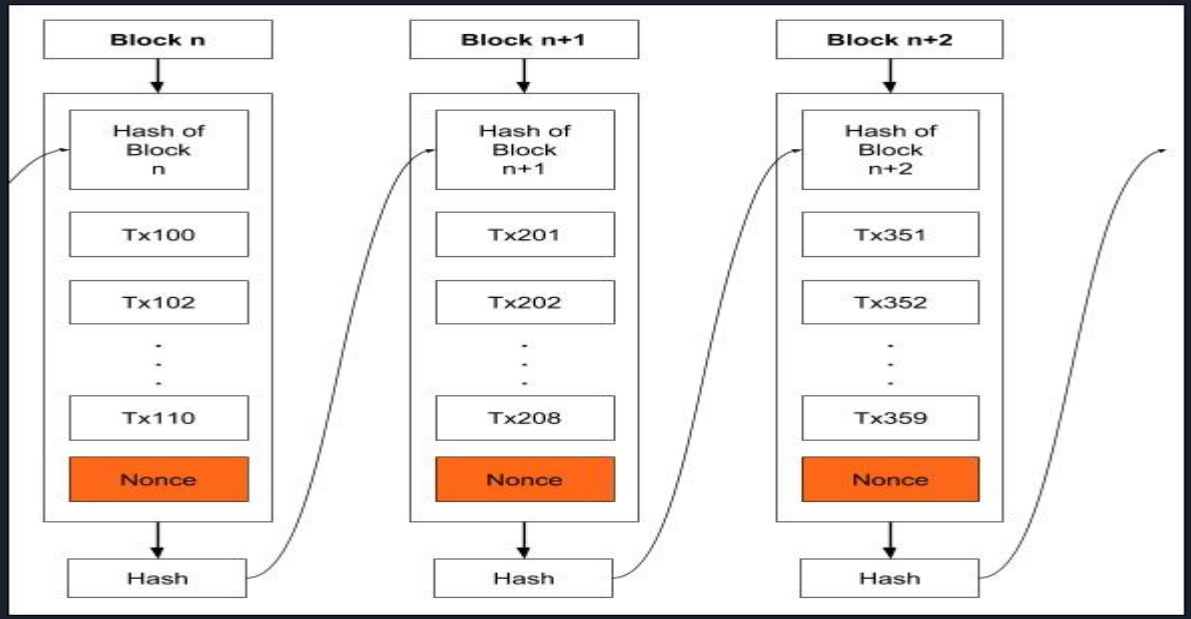
To each block, we now add one more item called Nonce.

Nonce is a number such that the block's hash meets a certain criterion. This criterion could be that the generated hash must have its leading four digits to be zero.Thus, the generated hash would look like 0000101010010xxx.

- Generally, the miner starts with a Nonce value of 0 and keeps on incrementing it until the generated hash meets the specified criterion.

Note: The hash generation works at random and is beyond your control - that is you cannot force the hash function to generate a certain hash. Thus, it may take several iterations until the desired hash with four leading zeros is generated.

The Bitcoin system awards the first successful miner by giving him certain bitcoins. If multiple people mine the block at the same time, then longest chain rule is followed (most work done).



Proof of Stake

Proof of stake

The probability of validating a new block is determined by how large of a stake a person hold.

The validators do not receive a block reward, instead they collect network fees as their reward.

Proof of stake systems can be much more cost and energy efficient than proof of work, but are less proven.

‘Proof of Work’ Vs ‘Proof of Stake’

Proof of Work	VS	Proof of Stake
 Mining capacity depends on computational power		 Validating capacity depends on the stake in the network
 Miners receive block rewards to solve a cryptographic puzzle		 Validators do not receive a block reward, instead, they collect transaction fees as reward
 Hackers would need to have a computer powerful than 51% of the network to add a malicious block, leading to 51% attack		 Hacker would need to own 51% of all the cryptocurrency on the network, which is practically impossible and therefore, making 51% attacks impossible.

But, we were talking about consensus algorithms. Why all of a sudden find a weird random number (nonce) or stake money?

BITCOIN

We define a bitcoin as a chain of digital signatures. Each owner transfers bitcoin to the next by digitally signing a hash of the previous transaction and the public key of the next owner and adding these to the end of the coin. A payee can verify the signatures to verify the chain of ownership.

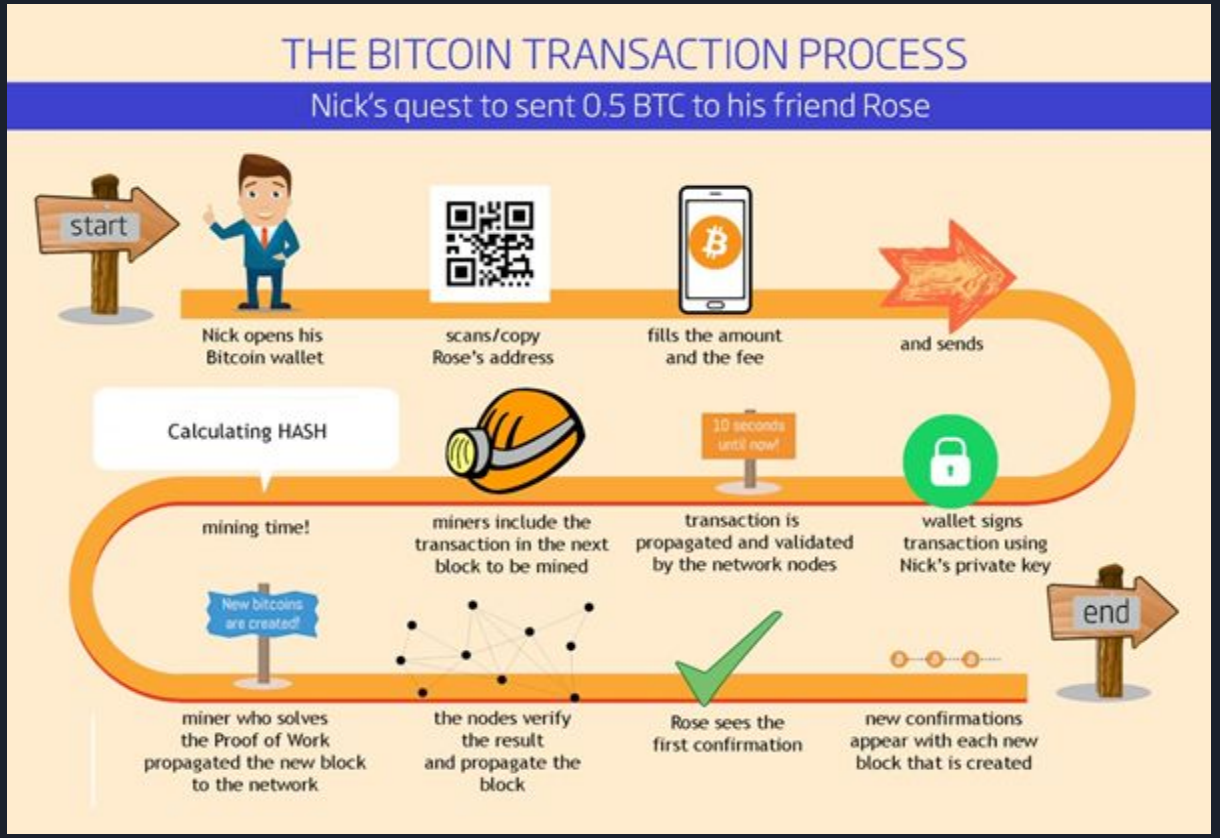
- Satoshi Nakamoto, BitCoin WhitePaper

Satoshi Nakamoto released BitCoin whitePaper in october 2008, and in january 2009, BitCoin was released for the public.

BitCoin leverages BlockChain technology and uses:

- SHA256 algorithm for encryption
- PoW consensus algorithm

BITCOIN Transaction Process



BITCOIN continued..

BitCoin was flourishing and the community was growing very fast.

In 2011, for the first time 1 BTC was equal to 1$. During the same time, a small teenager was keenly interested in BitCoin as a technology and started writing Blogs for it.

In the meantime, he suggested, If BitCoin is so awesome and secured, why are we using it just for ‘payment settlements’. Why not we execute some complex logics too in the same secured environment.

His idea was not much accepted. It seemed like…. He will give up.

Vitalik Buterin (Pushpa Bhau)

{Mai Jhukega nhi saala}

Ethereum

Vitalik initiated the project ‘Ethereum’, which was based on BlockChain Technology. But, with an important modification, you can now write complex programs and logics and deploy them on the Ethereum BlockChain and the program will be immutable and you won’t be able to make changes in it afterwards.

~> It is uses **PoS (proof of stake)** consensus algorithm.

Gas fees:

In Ethereum the programs that you’ll write, will be executed on all the node (all the participants in the network). So, they will be using their resources for your program. Hence, you need to incentivise them to do so. Therefore, you’ll pay them some extra ‘ethers’. This is called ‘Gas fees’.

Smart-Contract

The immutable programs that we can deploy on Ethereum BlockChains are called ‘Smart-Contracts’.

- It is written in Solidity language.
- It is a compiled, turing complete & object-oriented language for writing smart-contracts.
- To write smart-contracts initially, you can use Remix ide.
- For paying gas fees, you need to have a wallet. We will use MetaMask for the hands on session.