Fundamentals of Blockchain

Blockchain

* Blockchain idea was initiated by two people - Stuart Haber and W. Scott Scornetta in 1991.

* Blockchain is a distributed immutable ledger which is completely transparent.

* Blockchain is called distributed because whenever a new block is created then all the systems/nodes connected to the network gets notified or shows the new block.

* It is transparent bcz any changes made in one node, then all the interconnected node can see the changes made in it. We can only see the Hash

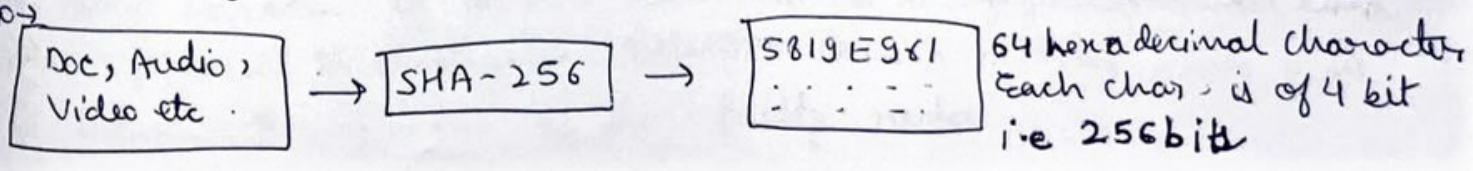
more features - Decentralized
- Transparent & Flexible
- Speed & Efficiency
- Security & Immutability
- Counterparty Risk Approval
- Trust Minimalized Aggreements

Applications - DeFi
DAOs
NFTs etc

Drawback - Technology cost - POW system consumes vast amount of computational power.
- Speed & Data Inefficiency - Takes about 10 mins to add a new block
- Illegal Activities

Hash functions - These are mathematical functions that transform or map a given set of data into a bit string of fixed size also known as "Hash value".

* Hash value is calculated by complex mathematical algorithms that convert data of arbitrary length to data of fixed length. [SHA-256 Algorithm]



Requirements of Hash Algorithm

① One way

Data ⟶ Encrypted Data

⟵ ✗

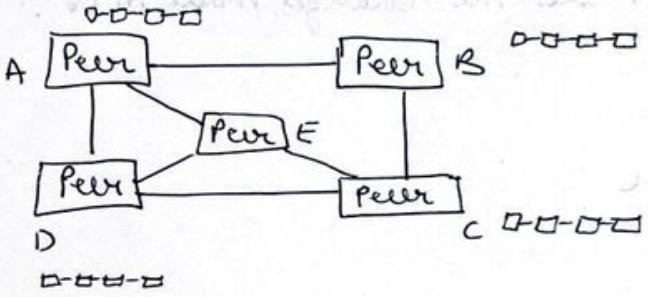
② Deterministic – Hash of two similar phase will always be same.

③ Fast Computation

④ Withstand Collisions → Hacker cannot hack

⑤ Avalanche Effect → If we make any change in the document, whole hash will change

Peer-To-Peer Network

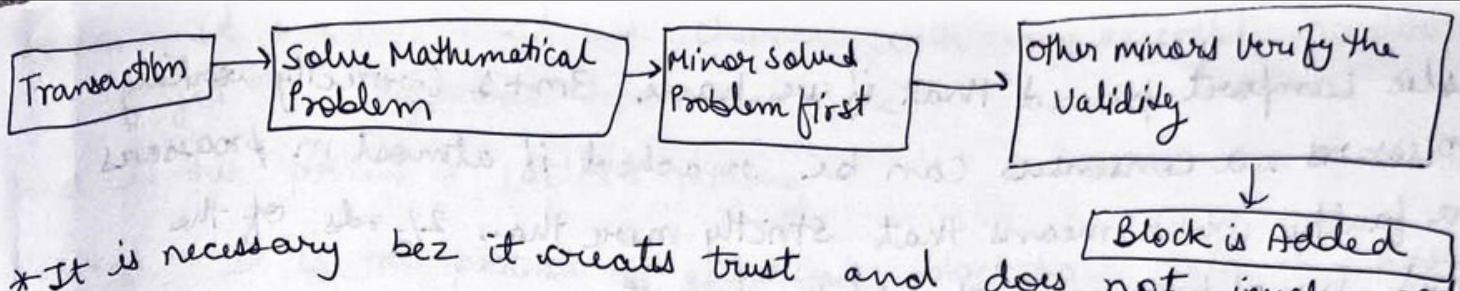


Blockchain Mining

Mempool – It is a place where group of miners are present & work on making the transaction happen.

* It acts as a sort of waiting room for transactions that have not yet been included in a block.

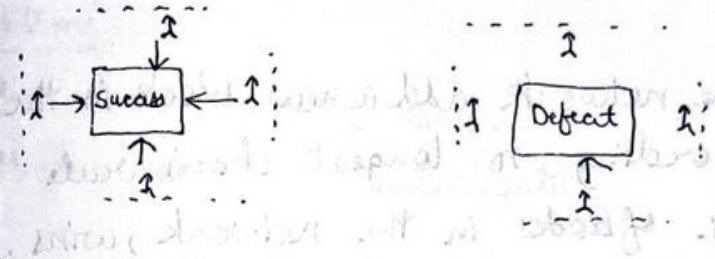
→ They pick each transaction from mempool & try to add that transaction into block. Each time they try to add it into block they have to solve a mathematical problem which is called PoW. And when it is solved, a new block is created. After creation of new block in order to attach it into block, miner have to let other miners know that he had solved a mathematical expression and created a new block. When other miners verify that the PoW is correct, they let add it into blockchain & in return miner received a reward that he added a block.



*It is necessary bez it creates trust and does not involve 3rd party.

Byzantine General Problem

"How do we make absolutely sure that multiple entities which are separated by distance, are in absolutely full agreement before an action is taken?"



Suppose a city is surrounded by armies on each side. And we need to attack at the same time. The city is strong enough to defend itself against one of our armies but not strong enough to defend against all four at the same time. If we don't attack at the same time we loose.

So, the generals of each army need to agree on the exact moment of when to attack. They communicate by sending messages back and fourth through the enemy city. The messenger could potentially get caught in the city and replaced by a fakenews messenger who will intentionally try to deceive the other general to attack the city at the wrong time, dooming our army to loose.

Byzantine Fault Tolerance

*BFT is a consensus algorithm introduced by Barbara Liskov and Miguel Castro.

*It is the feature of a distributed network to reach consensus even when some of the nodes in a network fail to respond or respond with incorrect information.

* The main objective of the BFT mechanism is to safeguard against the system failures by employing collective dicision making which aims to reduce to influence of the faulty nodes.

* Leslie Lamport proved that if we have $3m+1$ correctly working processors, a consensus can be reached if atmost m processors are faulty which means that strictly more than $2/3^{rds}$ of the total no. of processors should be honest.

Consensus Protocols

* blocks which are rejected during completing chain problem are called Orphan Blocks

They prevent us from two things –
- prevent attacks
- Competing chain problem

↓

Suppose two nodes of the same network add a new block in the blockchain at same time. According to longest chain rule the one who has the majority of blocks in the network, wins.

* The consensus protocols of Blockchain is much better than the Byzantine Fault Tolerance as consensus protocol only needs a 51% majority while Byzantine Fault Tolerance needs approximately 66%.

Types of Consensus protocols

1. Proof of Work (PoW)

* It requires that a miner uses some of his resources i.e computing power to hash the block's data until a solution to the mathematical ~~solution~~ problem is found.
* Hashing the block's data means that you pass (i/p data) it through a hashing function to generate a block hash.
* The reverse is impossible i.e we cannot pass block hash as input to get the input data.
* In PoW, we must provide data to whose hash matches certain conditions if it does not we have to change our data slightly to get the different hash.
* To get different hash each time, we ~~add~~ add a piece of information that is variable/random otherwise we get the same hash as o/p everytime [Nonce]

nonce - It is a no. that we change with every attempt inorder to get the different hash each time.

And all this process is called mining.

Mining - It is the process of gathering blockchain data and hashing it along with a nonce untill you find a particular hash..

* If we find the hash that satisfies the conditions set out by the protocol we get the right to broadcast the new block to the network.
* Now, other participants / miners verify the new block and update the blockchain by including the new block.

Problems -

1. Increased energy usage
2. Mining pools → centralization

Proof of Stake (PoS)

* Here, it uses an election process in which 1 node is randomly chosen to validate the next block.
* There are no miners but Validators and does not let people mine new blocks but forge / mint new blocks.
* Validators are not choosen randomly, to become a validator, a node has to deposit (lock) a certain amount of coins into the network as stake (security deposit)
* The size of the stake determines the chances of a validator to be choosen to forge the next block.
* Unique methods like Randomized block Selection, Coin Age Selection are added into the selection process to favor not just the wealthiest nodes in the network.

Randomized Block selection :- Here validators are selected looking for nodes with a combination of the lowest hash value and highest stake.

* Since sizes of stakes are public, next forger can easily be predicted.

Coin Age Selection - This method chooses nodes based on how long their tokens have been staked.

Coin Age = no. of days the coins have been staked X no. of coins staked

* Once a node has forged a block, its coin age is set to zero & it must wait a certain period to forge another block - This prevents large stake nodes from dominating the blockchain

→ when a node gets chosen to forge the next block, it will check if the transactions in the block are valid & then signs and add it to the blockchain.

→ As a reward, the node receives the transaction fees or a coin reward

Bitcoin

* by Satoshi Nakamoto

Bitcoin's Monetary Policy

* To ~~st~~ maintain supply of money / currency

Principles -

1. The Halving
2. Block Frequency - This states that on an avg. it will take 10 min. to create new block

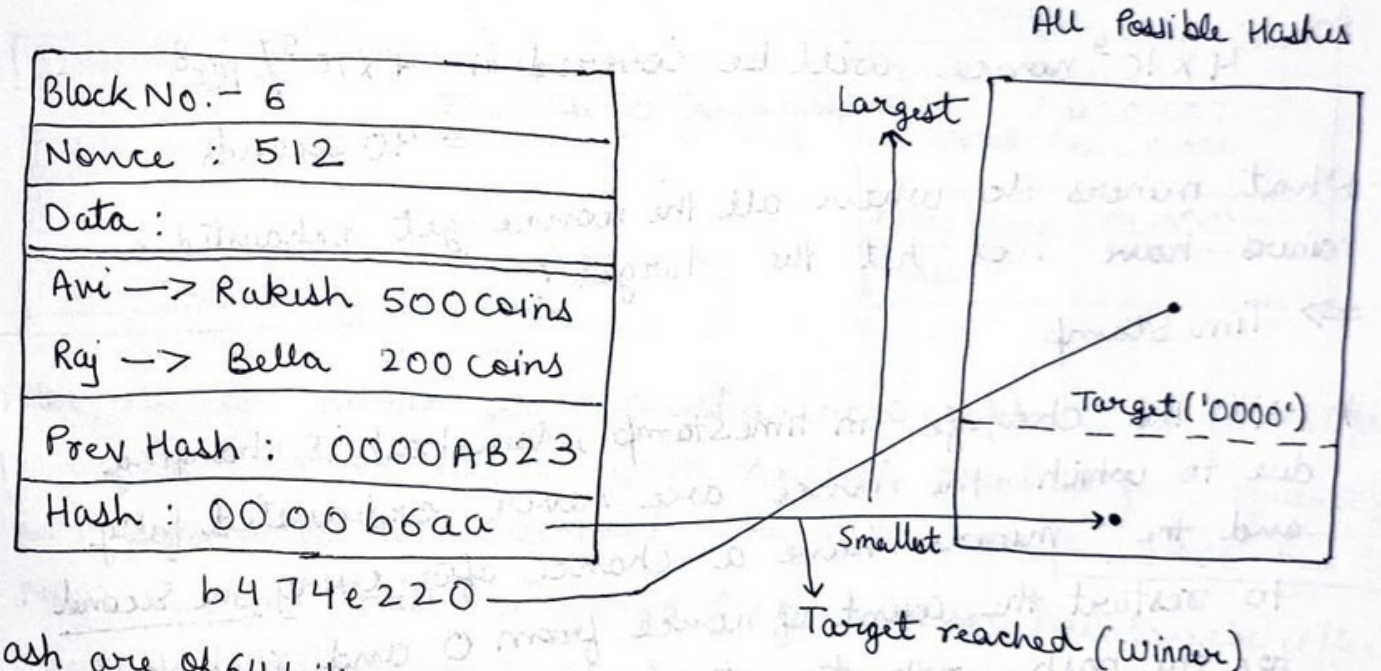
Halving - After every 210,000 blocks mined or roughly every four years, the block reward given to the Bitcoin miners for processing transactions is cut in half. This event is referred to as halving because it cuts the rate at which new bitcoins are released into circulation.

Launch of bitcoin	03 Jan, 2009	0	50 new XBT
1st halving	28 NOV, 2012	210,000	25 new XBT
⋮	⋮	⋮	⋮
max supply reached	Expected 2140	6 9 30000	0 new XBT

How Mining Works?

1. Nonce – It is the number that blockchain miners are solving for. (It is a 32 bit number)

2. Target :- * It is a number used in mining.
   * It is a number that a block hash must be below for the block to be added on to the blockchain.
   * The target adjusts every 2016 blocks (roughly two weeks) to try and ensure that blocks are mined once every 10 minutes on average.



* Hash are of 64 bits.

CPUs Vs GPUs Vs ASICs

CPU < 10 MH/s

GPU < 1 GH/s

ASIC > 1000 GH/s

H/s → Hashes / sec

Mining Pool – It is a joint group of cryptocurrency miners who combine their computational resources over a network to strengthen the probability of finding a block.

* Rewards are usually divided between the individuals who contributed according to each individual's processing work/power.

Nonce Range

* Nonce is a 32-bit number

Range of Nonce = 0 to $2^{32} - 1 \simeq 0$ to 4×10^9 (4 Billion)

Total no. of possible hashes –

$16 \times 16 \times 16 \ldots \ldots$ (64 times) $\ldots 16 = 16^{64} \simeq 10^{77}$

* There are not enough nonce to generate the valid hash.

* A modest miner does 10^8 hashes/sec

So, 4×10^9 nonce will be covered in $4 \times 10^9 / 10^8$

$= 40$ seconds

Q. What miners do when all the nonce get exhausted & miners have not hit the target?

⇒ TimeStamp

* With the change in timestamp, Our hash is changing due to which the nonce are never exhausted fully and the miners have a chance after every one second to restart the count of nonce from 0 and recheck for the hash with target.

Block No: 1
Nonce :
TimeStamp : 1622114685
Data
Prev Hash : 0000000
Hash

* Current hashing rate is 231.428 million trillion hashes/sec

So, all nonce are covered in = $4 \times 10^9 / 10^6 \times 10^{12} = 4 \times 10^{-9}$ s

4×10^{-9} sec <<<< 1 sec

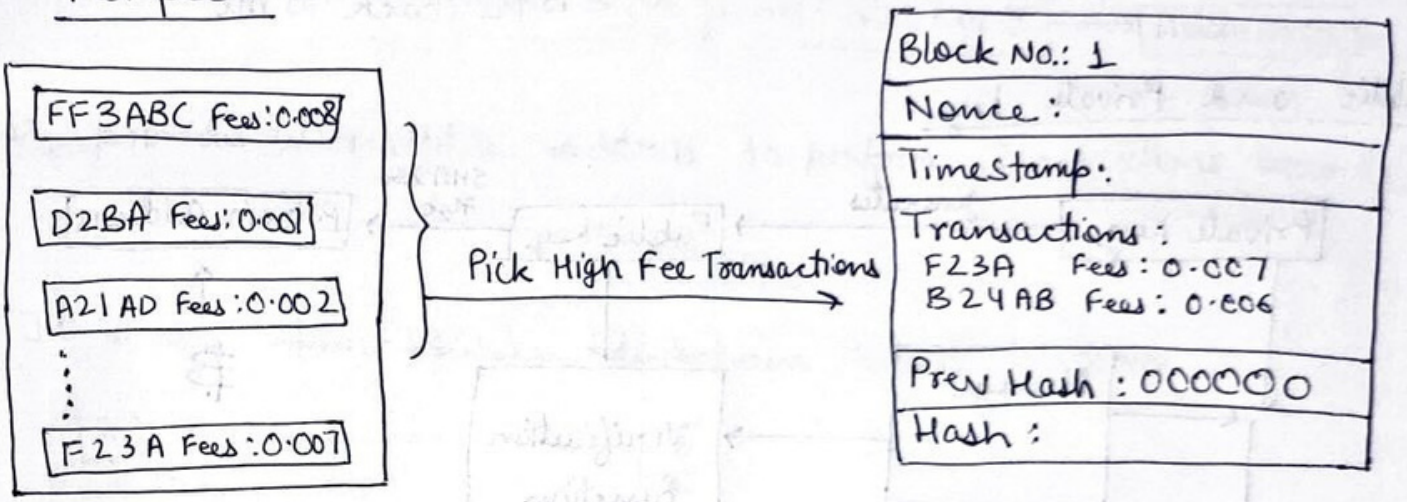
Q. What should the miners do in idle time? Should they wait for timestamp to change?

⇒ NO, Here comes Mempool –

Mempool – It is an area where group of miners are present and work on making the transaction happen.

* It acts as a sort of waiting room for transactions that have not yet been included in a block.

Mempool



After all the nonce gets exhausted, now replace the lowest fee transaction in the block with the just smallest fee (adjisent fee no.) present in the mempool. Like in this case, F23A6C Fees: 0.005 Now, a new Hash is formed due to change / avalanche effect. Hence the nonce will start again from 0 and this process goes endless until the target is reached.

Transactions and UTXOs

UTXO – An Unspent transaction output (UTXO) is the technical term for the amount of digital currency that remains after a cryptocurrency transaction.

eg:

Arjun → Me 0.4 BTC
Raj → Me 0.3 BTC
Alice → Me 0.7 BTC
Bob → Me 0.1 BTC
} UTXOs

Lets say I buy coffee for 0.5 BTC

Transaction

Pick an amount from UTXOs which is greater or equal to the amount of coffee i.e 0.5BTC

Input:

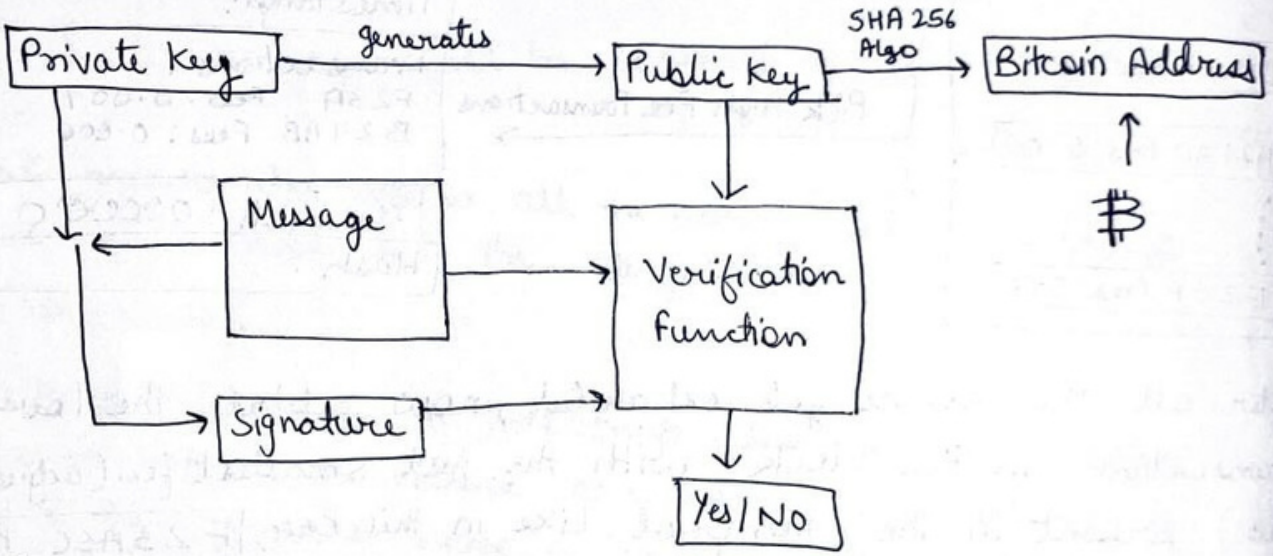
0.7BTC from Alice

Output

0.5BTC to the Coffee Shop

0.2BTC back to me

Public and Private key

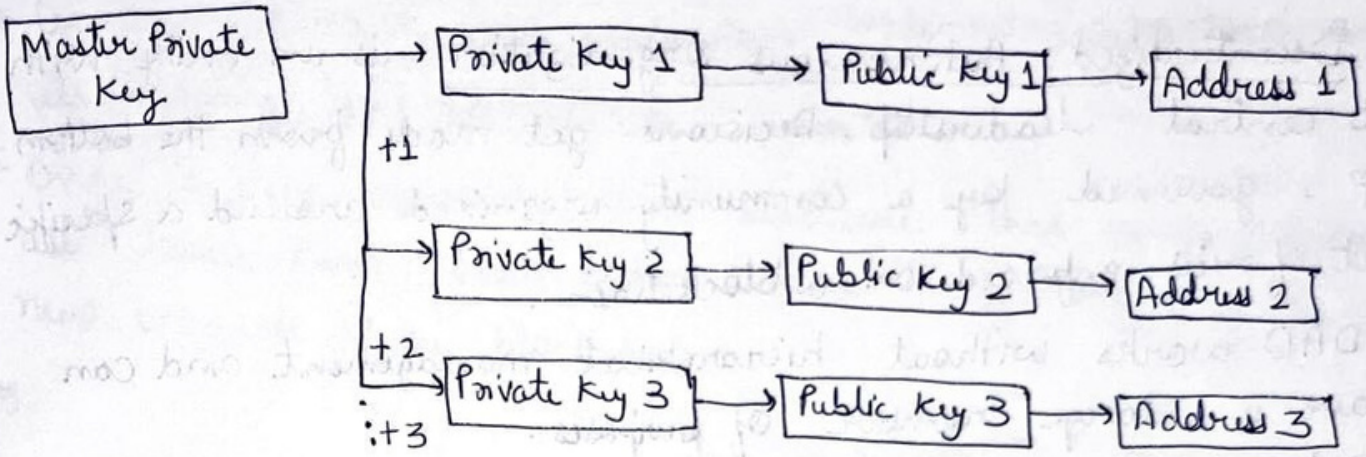


* To verify that the transactions are performed by me or not.
* Signature is the combination of private key and message.
* Public key is used when we want to perform transaction.
* Bitcoin Address is used by others to send money to us.

Segregated Witness

* Earlier the size of each block in the blockchain was 1MB for storing of the Transactions.
* So, the transaction speed was reduced. In order to overcome this, the community decided to remove signature and Public key from each transaction information. This was occupying 60-65% of space.
* Since these witness features (sig. & Public key) were removed from the input field of the block, helped to solve a blockchain size limitation problem.

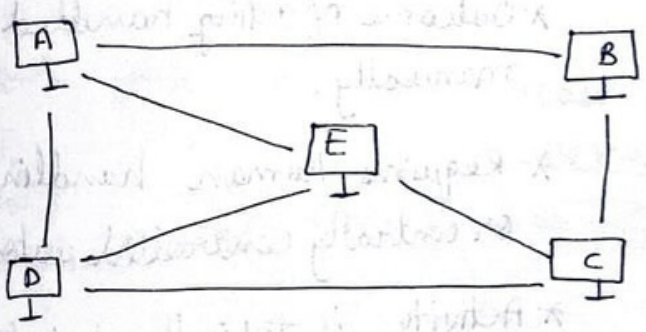
Hierarchically Deterministic (HD) Wallets :-



* It provides us multiple address to perform transactions securely.

Ethereum

* It is an open-source blockchain based platform.



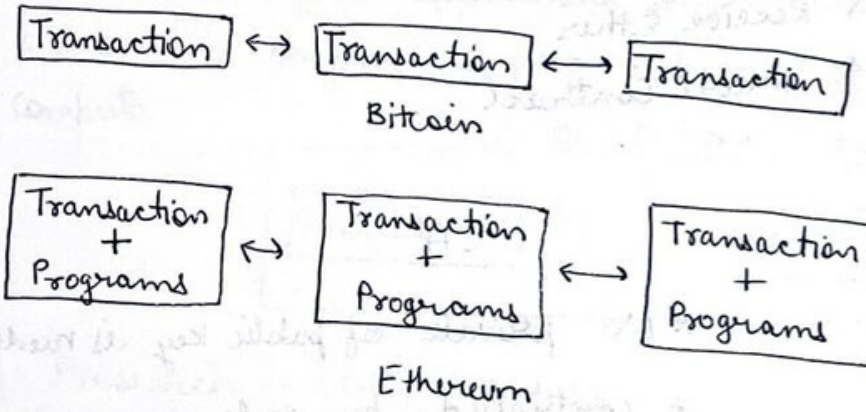
Types of Nodes

1. Full Node : Locally stores a copy of the entire blockchain
2. Light Node : * Stores only the block header.
   * Depends on full node
   * Simply to perform transactions
   * For low capacity devices which cannot afford to store the gigabytes of data.
3. Archive node : * Stores everything kept in the full node and built an archive of historical data.
   * Requires terabytes of disk space.

Blockchain

* A blockchain is a distributed immutable ledger
* A ledger is a place where transactions are recorded.
* The block of the blockchain is used as a ledger.
* It is in peer-to-peer network where each block/host has same amount of data present.
* A miner is a person who mines a particular block and creates a block.

Ethereum [Vitalik Buterin]



1. Decentralized
2. Transparency & Flexible
3. Speed & Efficiency
4. Security & Immutability
5. Counterparty Risk removal
6. Trust Minimized Agreements

Applications

1. Decentralized finance DeFi
2. DAOs (Decentralized Autonomous Organizations)
3. NFTs

* This enabled Decenteralised Applications (DApps)
* Ethereum is an open-source blockchain based platform

Technology : Blockchain

Protocol/Coin : Ethereum Bitcoin Wave Neo (like we have https/http (define rules))

Token : TRX SNT WGT B1 DBC TKY
REP AE X WCT INTL ONT TNC

Ethereum Account

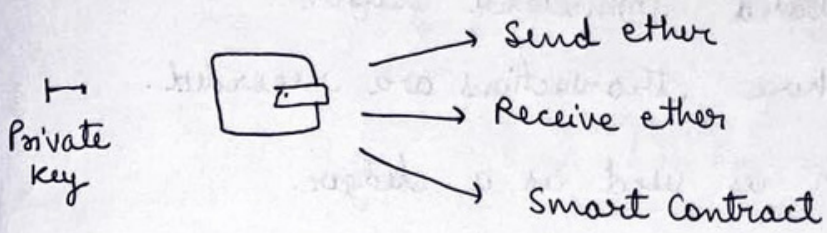
* An Ethereum Account is an entity with an ether (ETH) balance that can send or receive transactions on Ethereum.

Two Types

1. Externally Owned Account (EOA)
2. Contract Account (CA)

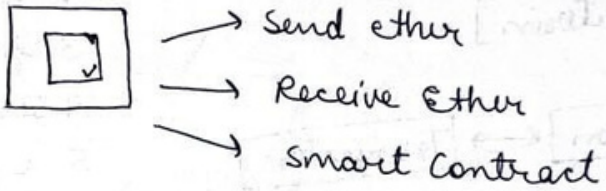
* Ethereum uses Keccak-256 as hashing algorithm ↓ SHA-256

EOA : (Like (eg): MetaMask)



CA :

A Contract Account is created whenever we deploy a smart contract on our Ethereum blockchain



EOA	CA
* Private key is needed	* No private of public key is needed
* Controlled by humans.	* Controlled by code.
* NO Gas is associated.	* Gas is associated
* Has a unique address.	* Has a unique address
* Holds ETH balance.	* Holds ETH balance.

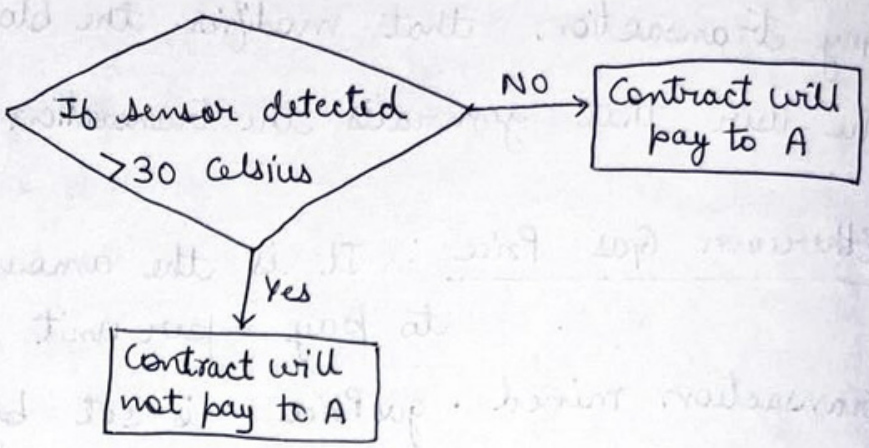
Smart Contract

* These are simply programs stored on a blockchain that run when predetermined conditions are met.

* They typically are used to automate the execution of an agreement so that all participants can be immediately certain amount of the outcome, without any intermediary's involvement or time loss.

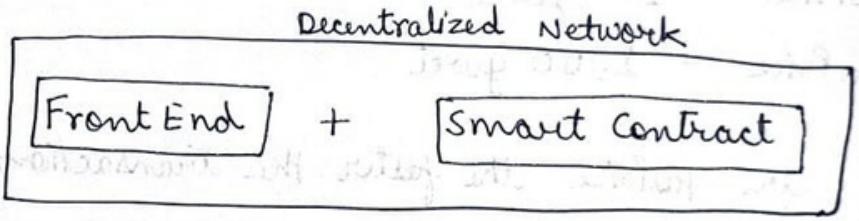
* farm and fruitseller example :

Smart contract:



Decentralized Applications [dApps]

* These are digital applications or programs that exist and run on a blockchain or peer-to-peer network of computers instead of a single computer.



eg: Presearch , LBRY , D.tube

Centralized Apps

* Not Trustworthy
* censorship
* You pay
* Can go down

Decentralized Apps

* Trustworthy
* No censorship
* They pay
* Cannot go down

Ethereum Virtual Machine (EVM)

* It is the software platform that developers can use to create DApps on Ethereum.
* It is used for executing smart Apps so that the chain is safe from hackers and virses.

Ethereum Gas :

* Any transaction that modifies the blockchain costs gas.
* The user that generates the transaction pays for the gas.

Ethereum Gas Price : It is the amount the sender wants to pay per unit of gas to get the transaction mined. gasPrice is set by the sender.

Gas Price is denoted in **gwei**

$$1 \text{ gwei} = 10^{-9} \text{ ETH}$$

eg: 1 gasPrice = 10 gwei
1 gasPrice = 1000 gwei

(IMP)
* The higher the gasPrice the faster the transaction will be mined.

Ethereum Gas Limit

* It is the maximum gas that the transaction can consume.
* It is set by the sender.

Transaction Fee = Gas units (limit) * (Base fee + Tip) OR ↓

Let us assume —
A has to pay B 1 Eth. What will be the transactionfee?

Gas limit for transaction = 21,000 units [standard]
Base Fee = 100 gwei
Tip = 10 gwei

Transaction fee = 21000 * (100+10) = 23,10,000 gwei
= 0.000231 ETH

Transaction Fee = Gas units (limit) * Gas price per unit

DAO

* A Decentralized Autonomous Organization is an entity with no central leadership. Decisions get made from the bottom-up, governed by a community organized around a specific set of rules enforced on a blockchain.
* A DAO works without hierarchical management and can have a large number of purposes.
** → ↓

DAO	vs	Organization
* Fully decentralized.		* Usually hierarchical
* Voting required		* Voting may or may not require
* NO trusted intermediary to count vote.		* Outcome of voting handled manually.
* Services offered are handled automatically.		* Requires human handling or centrally controlled automation
* All activities are transparent and fully public.		* Activity is typically private & limited to the public.

The DAO - It was an early iteration of modern DAOs. It was launched back in 2016 and designed to be an automated organization that acted as a form of venture capital fund.

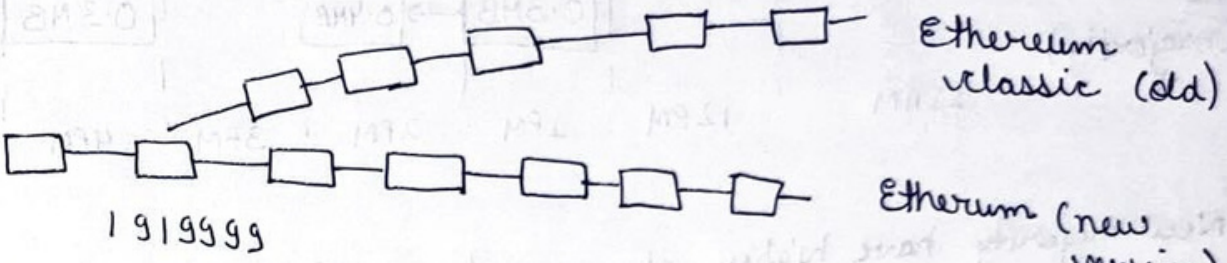
The DAO Attack -

** DAOs goal is to codify the rules and decisionmaking apparatus of an organization, eliminating the need for documents and people in governing, creating a structure with decentralized control.

Hard Fork

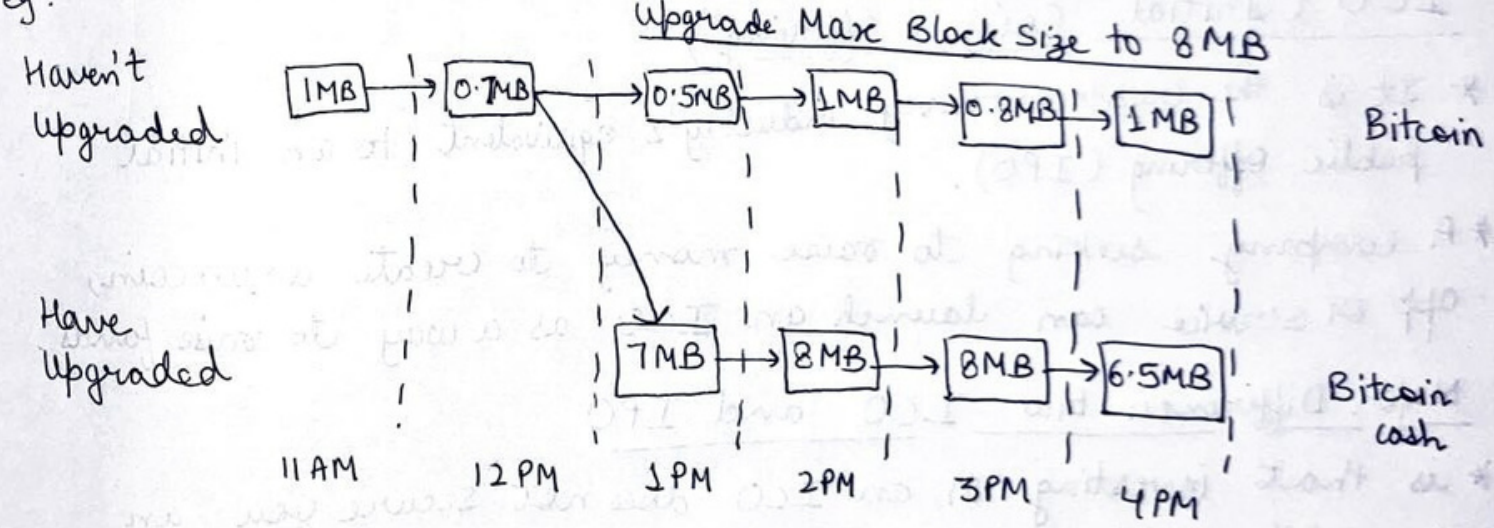
* During a hard fork, software implementing a protocol and its mining procedures is upgraded.
* Once a user upgrades their software, that version rejects all transactions from older software, effectively creating a new branch of the blockchain.

eg:



* However, those users who retain the old software continue to process transactions
* Hard fork was seen incase of Bitcoin also.

eg:

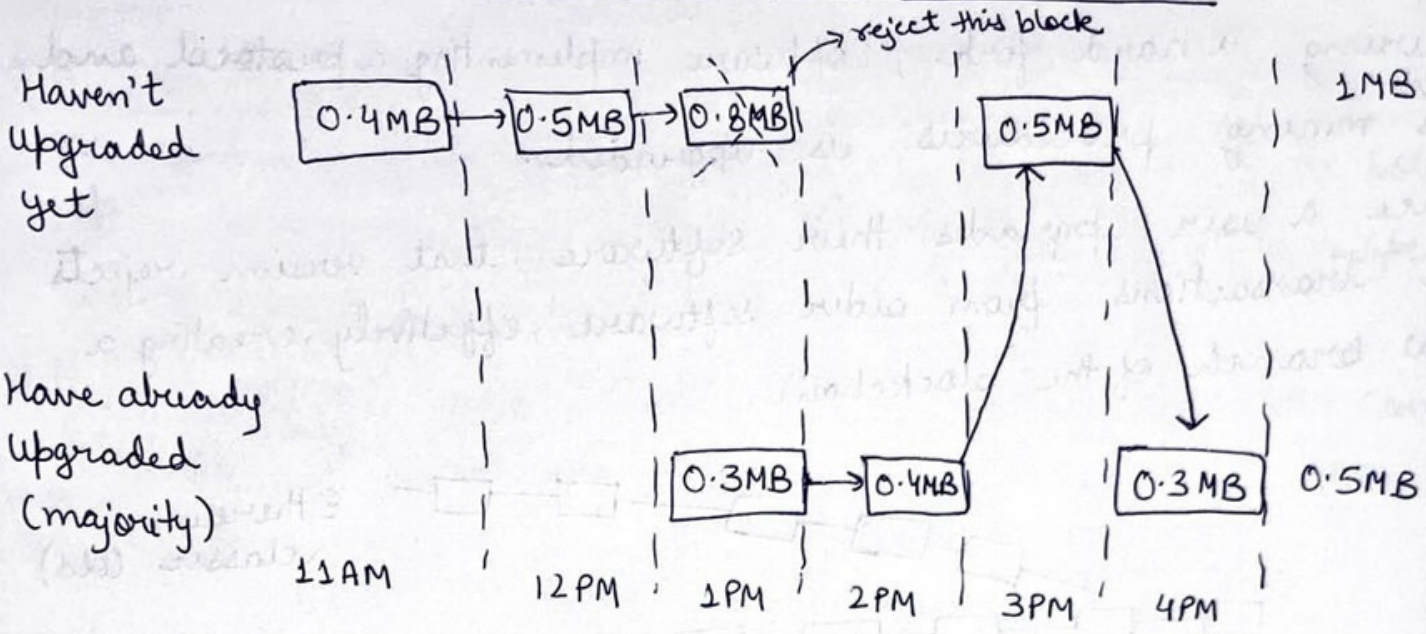


Soft Fork

* Soft forks are a change to the protocol, but the end product remains unchanged.
* A soft fork is a backward-compatible upgrade, meaning that the upgraded nodes can still communicate with the non-upgraded ones.
* Old nodes (not upgraded nodes) could still validate blocks and transactions, but they just wouldn't understand them.

eg:

Decrease block size to 0.5 MB



* New majority have higher chances for mining new nodes
* NO splitting in chain or ~~no~~ new branches.
* It becomes necessary for older version to upgrade themselves.

ICO (Initial Coin Offering)

* It is the cryptocurrency industry's equivalent to an initial public offering (IPO).
* A company seeking to raise money to create a new coin, app or service can launch an ICO as a way to raise funds.

Major Difference b/w ICO and IPO

* is that investing in an ICO does not secure you an ownership stake in the crypto project/company
* They deal in Tokens.
* They have less legal work.

Sharding - It is a database partitioning technique used by blockchain companies with the purpose of scalability, enabling them to process more transactions per second.

Thank You.