Blockchain: CE

@ Deepankar Sharma

Wednesday, December 14, 2022
6:12 PM

① Blockchain → Hashing → Immutable Ledger → Distributed P2P → Mining → Consensus
② Cryptocurrency → Bitcoin → Monetary Policy → Mining → Nonce → Machines
③ Smart contract
↳ Ethereum → Smart contracts → Dapps

Machines → Mempool → Transactions → wallets → Public key & Private key

Dapps → EVM & Gas → DAOs → Hard & Soft fork → DAO Attack → ICO
↳ Alt coins

- Stuart Haber
- W. Scott Stornetta

} # 1991 paper

Blockchain is a disruptive technology

* Internet → Communication
* Blockchain → Trust

Blockchain is a distributable immutable ledger, which is completely transparent.

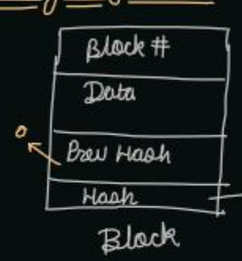
Applications

① Product Tracking
② Smart Contract

Sender Bank → Correspondent Bank → Receiver Bank

③ International Wire Transfer
④ Healthcare System

Hashing Algorithm



Genesis Block

Fingerprint of the Block → SHA256

Requirements of Hashing Algorithm

① One way
② Deterministic
③ Fast Computation
④ Withstand Collisions
⑤ Avalanche Effect

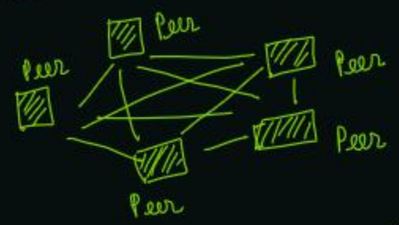
Immutable Ledger

Suppose buying a house

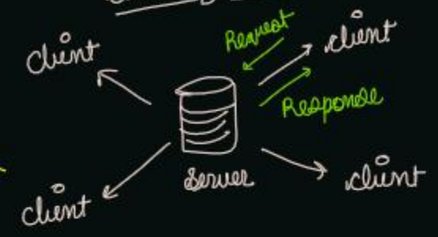
you → Money → Sales Deed → Institution → House

Institution → government → centralized database → Not transparent

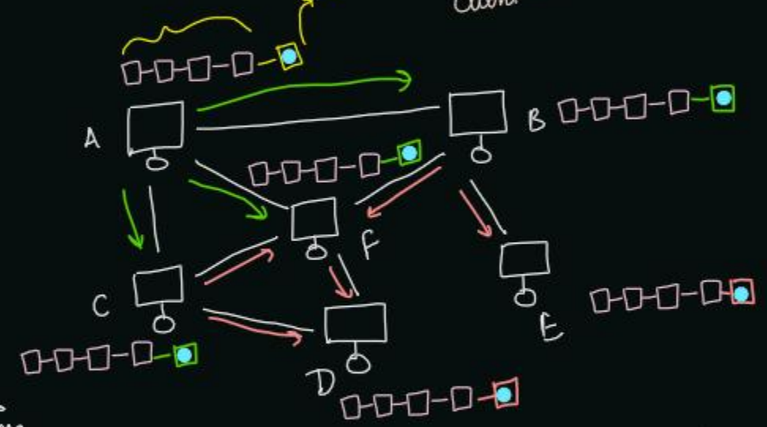
P2P Network (Distributed Peer 2 Peer Network)



Centralized Network



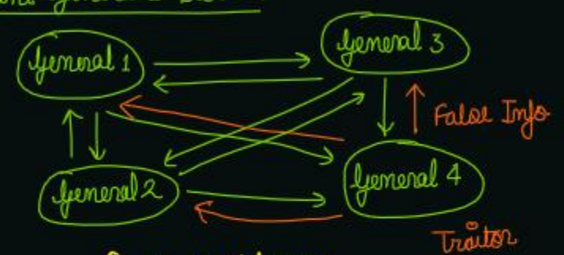
Blockchain :-



Blockchain Mining

Problem in Distributed Computing :

Byzantine Generals Problem



Practical Byzantine fault Tolerance

→ Miguel Castro

if 1/3 nodes support vulnerability, Follow majority (2/3 nodes)

Consensus Protocol

→ Prevent attacks → competing chain problem

↳ Two nodes mined new blocks at same time, conflict in Network

Types of consensus protocol :

① Proof of Work (POW)

New mined block

"Network will only accept the longer Blockchain, other mined block will be discarded"

Now longer chain is "ABCDFO" ← so network will accept it!!

- Byzantine Fault Tolerance needs approx 66% majority.
  Consensus Protocol only needs 51% majority ☺
- Orphan Block gets dropped, & miner don't get any reward for it.
- Wait for 6 confirmations before assuming payment is successful.
  → addition of 5 more blocks

Bitcoin

coinmarketcap.com

① Technology → Blockchain
② Protocol / coin → Bitcoin (X → No Token), Waves, Ethereum
③ Token →

WGB	BI
INTL	WGR

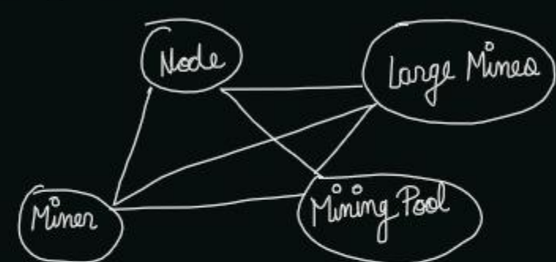
Waves

TRX	SNT
REP	AE

Ethereum

Founder of Bitcoin → Satoshi Nakamoto

Bitcoin Ecosystem →



Bitcoin's Monetary Policy

① The Halving

halving in every 4 years

Year	# Block	Reward
2009	0	50 new XBT
2012	210,000	25 new XBT

② Block Frequency

This states that on an average it will take 10 minutes to create a new block

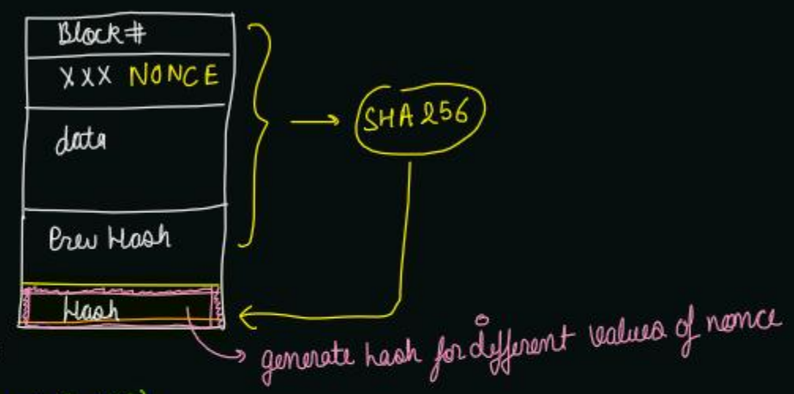
Blockchain.com

Supply cap of Bitcoin is 21 million
(Hyperinflation)

The Nonce

→ Solving the mathematical problem.

→ generate hash by altering the values of NONCE until $\boxed{\text{Target value}}$ is reached.

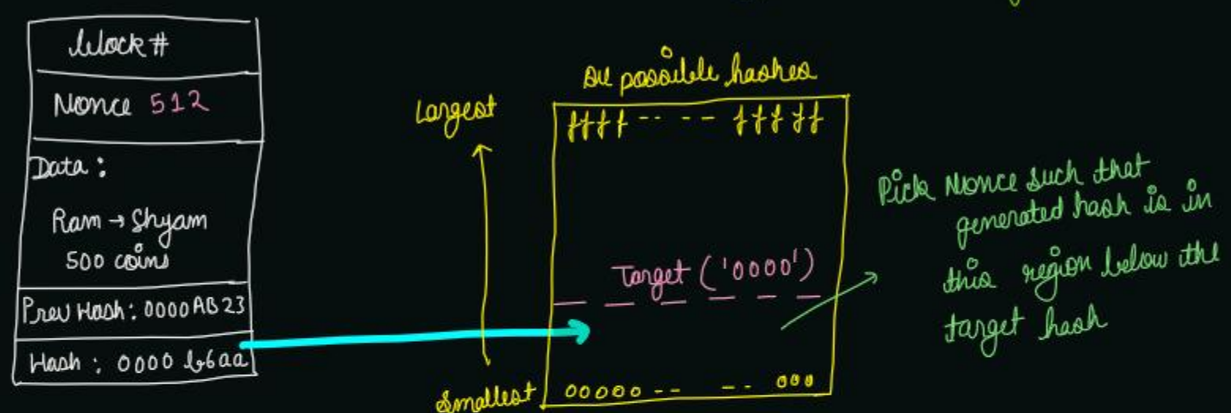


(demoblockchain.org)

Nonce: Nonce is the number that blockchain miners are solving for.

Target: Target 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 2 weeks) to try and ensure that blocks are mined once every 10 minutes on average.

data → (SHA-256) → 64 hexadecimal character
↳ each character = 4 bits
$64 * 4 = 256$ bits fixed output

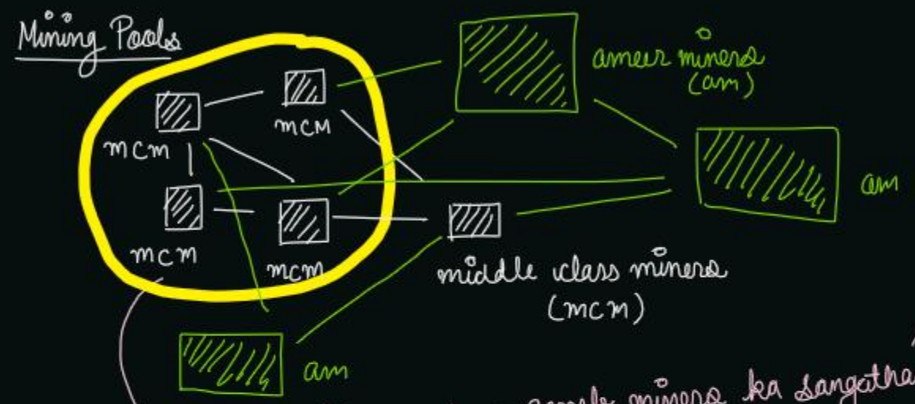


Target History

↳ to maintain the average of 1 block/10 minutes target is maintained by another algorithm.

ASICs → 1000GH/s → 1000 giga hashes/sec

Mining Pools



Mining pool → garib miners ka sangathan, to compete with ameer miners

↳ Basically group of miners, which later distribute the prize

→ divide nonce range

Nonce Range

Block #
Nonce
Data
Prev Hash
Hash

→ Nonce is 32 bit number

Range of Nonce = 0 to $2^{32} \approx 4 * 10^9 \approx$ 4 billion

Total possible hashes = $\boxed{\text{SHA-256}}$ → 256 bits

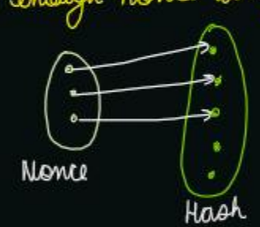
↳ $2^{256} = 16^{64} \simeq 10^{77}$ hashes

Total valid hashes $\approx 10^{77}$

Total Nonce we can generate $\approx 4 * 10^9$

$10^{77} >>>> 4 * 10^9$

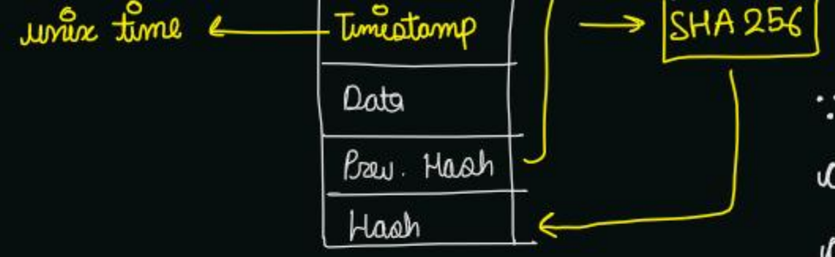
There are not enough nonce to generate the valid hash



- A modest mine does 10^8 hashes/sec
- $4 * 10^9$ nonces will be covered in

$$\frac{4 * 10^9}{10^8} = 40 \text{ sec}$$

So what will the miners do when all the nonce are exhausted & target not hit yet?



1 sec → 0.1 billion nonce

∵ every second timestamp is changing, so miner won't be able to exhaust nonces

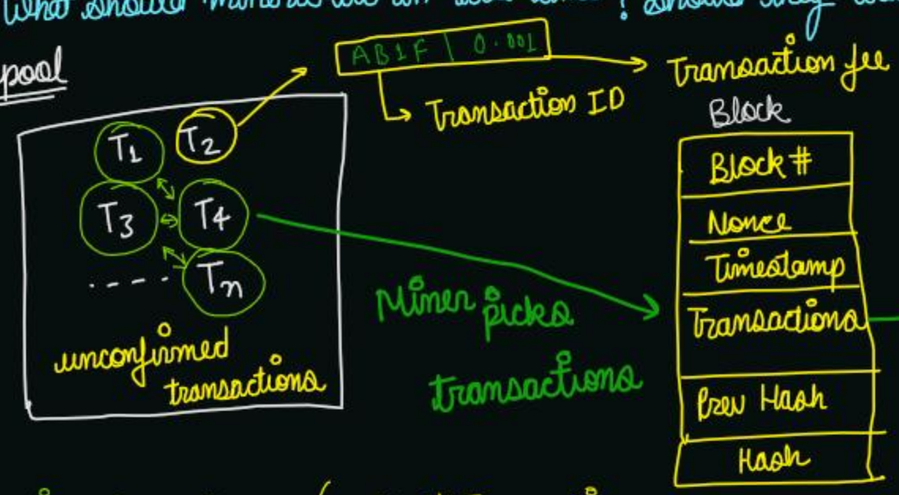
current hashing rate ≈ 180 million trillion hashes/sec.

So $4 * 10^9$ nonces will exhaust in $4 * 10^{-9}$ sec

$$\frac{4 * 10^9}{10^6 * 10^{12}} = \underbrace{4 * 10^{-9} \text{ sec}}_{\text{timestamp change hone se pehle hi}} <<<< 1 \text{ sec}$$

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

Mempool



{ T_1, T_3, T_4, T_n } change transactions if Nonce is exhausted & timestamp hasn't changed

Transactions & UTXOs → (unspent Transaction Output)

UTXO → amount of cryptocurrency left with someone after transaction.

Arjun → Me	0.4 BTC	UTXOs
Raj → Me	0.3 BTC	
~~Alice → Me~~	~~0.7 BTC~~	
Bob → Me	0.1 BTC	
Me → Me	0.1 ~~0.2~~ BTC	

Purchase item for 0.5 BTC

Transaction:

0.7 BTC from Alice (Input) → 0.5 BTC to owner of item (Output) ← UTXO of owner

→ 0.2 BTC back to me

Transaction fee

↳ sent to miner

Block 1 Block 2 Block 3 Block 4

Alice → Me 0.7 BTC

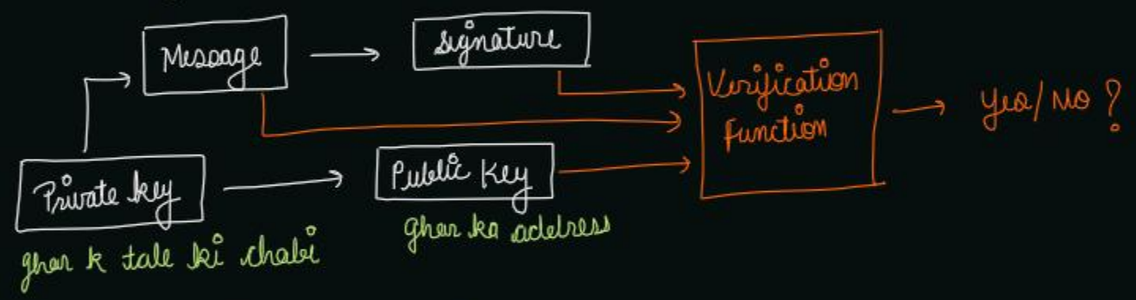
Bob → Me 0.4 BTC

Me → Coffee 0.5 BTC

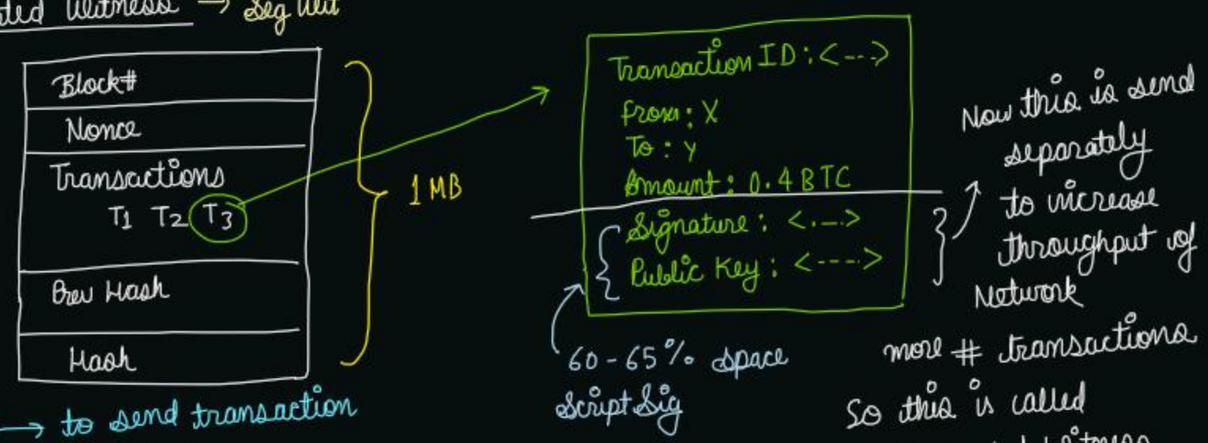
Me → Me 0.2 BTC

Wallet adds these UTXOs and ⇒ gives balance 0.6 BTC
fetches

Public key & Private Key (tools · supordata science)



Segregated witness → Seg wit



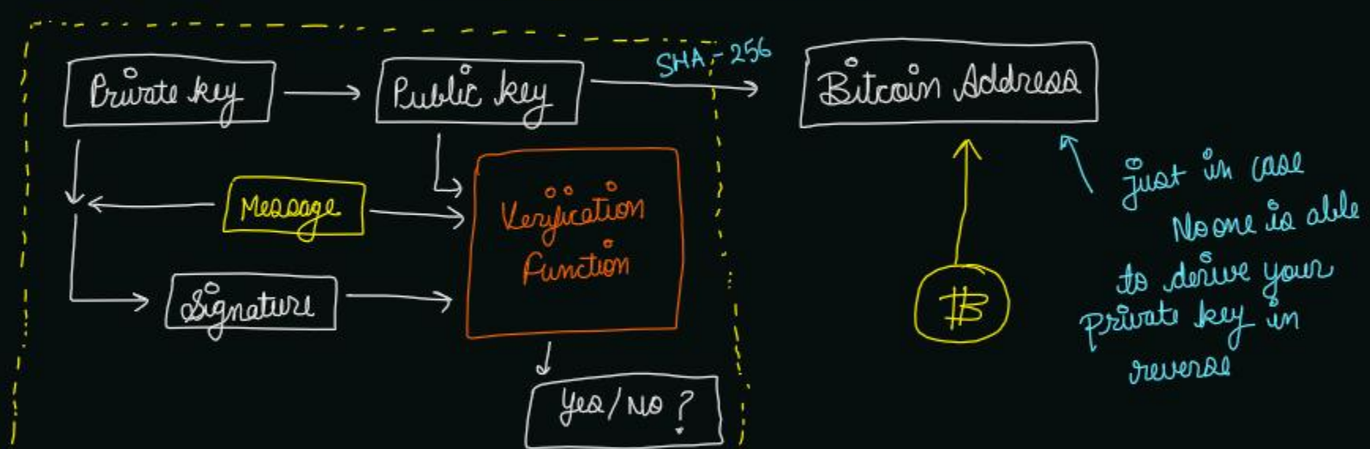
Now this is send separately to increase throughput of Network

more # transactions So this is called Segregated Witness.

Public key V/S Bitcoin Address

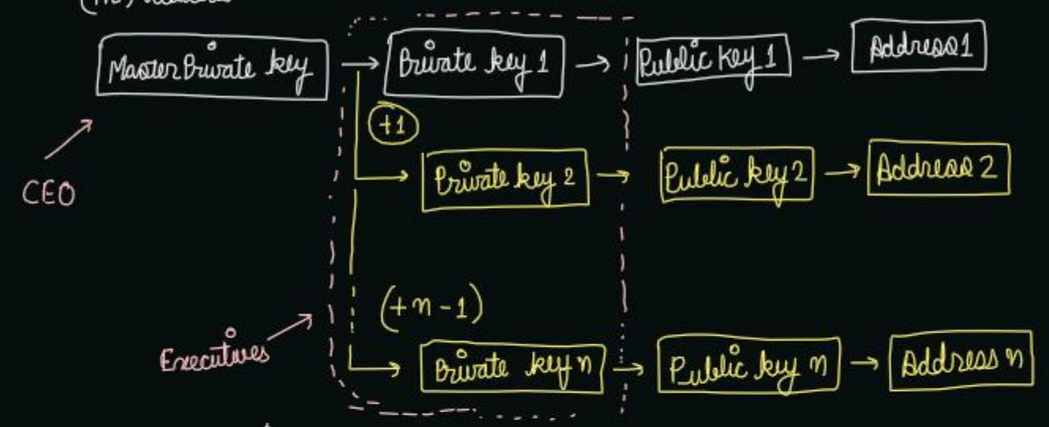
to send transaction

to receive transaction



Just in case No one is able to derive your private key in reverse

(HD) Wallets



Ethereum

→ Ethereum is an opensource blockchain-based platform.
→ distributed immutable ledger

- → Vitalik Buterin (19 years) → 2013
- → Smart contracts → daapa
- → Ethers (cryptocurrency)

Ethereum Nodes

Types of Nodes

Miners →

1. Full Node → verifies & validates all the block → locally stores a copy of entire blockchain
2. Light Node → stores only block header. Depends on full Node
   - → For low capacity devices which can't afford to store gigabytes of data
3. Archive Node → stores everything in the full node and built an archive of historical data.
   - → requires terabytes of disk space.

Accounts in Ethereum

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

private key + Wallet → send / receive transaction
→ Smart contract
→ check balance

Types of Ethereum Accounts

1. Externally Owned Account (EOA)
2. Contract Account (CA)
   - → controlled by the contract code

→ No Gas is associated
→ Has a unique address
→ Holds ETH balance

→ Gas is associated
→ Has a unique address
→ Holds ETH balance

Smart contract

Bitcoin → Bitcoin script (Not Turing Complete) loops X → infinite loops may cause trouble

Ethereum → Solidity (Turing complete) loops ✓ ☺

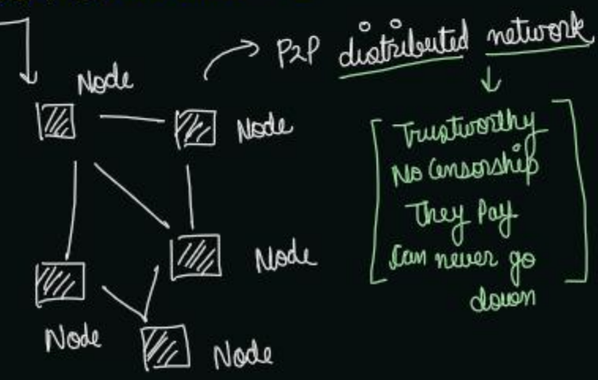
↳ fully qualified like programming language

↳ more execution → more gas fees → reduce execution time

Each node has the following :

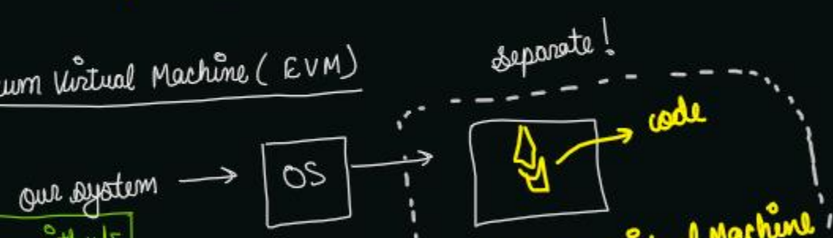
1. Current state of all smart contracts
2. History of both transaction and smart contract.

Decentralized Applications (Daapps) → Front End + Smart Contract (Backend)



	Centralized Apps		Decentralized Apps
Search Engine	Google	→	Presearch
Social Media	Facebook	→	LBRY
Video Platform	YouTube	→	D Tube

Ethereum Virtual Machine (EVM)



↳ 5 gas ↳ 3 gas ↳ 3 gas

① Any transaction that modifies the blockchain costs gas.
② The user that generated the transaction pays for the gas.

Gas Price → It is the amount, the sender wants to pay per unit of gas to get the transaction mined.
- ↳ Gas price is set by the sender.
- ↳ Gas prices are denoted in gwei ($1 \text{ gwei} = 10^{-9}$ ETH)

$\boxed{1 \text{ gas} = 100 \text{ gwei}}$ ← set by the sender

The higher the gas price, the faster the transaction will be mined.

Ethereum Gas Limit →

Gas Limit → maximum gas a transaction can consume
↳ set by the sender

A ⟶ B, what will be the total fee? (2 ETH) → A sets gas price/unit = 100 gwei, Transaction gas limit = 21,000 units

$\boxed{\text{Total fee} = \text{Gas units (limit)} * \text{Gas price per unit}}$ → 21,000 * 100 = 21,00,000 gwei = 0.0021 ETH

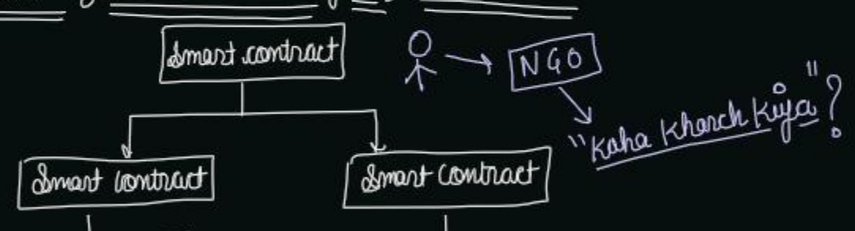
If A sets transaction gas limit < 21,000
for example 20,000 ↳ this is gone too!
$\boxed{\text{Transaction Failed}}$

A sets Transaction gas limit > 21,000
for example 22,000
22,000 − 21,000 = $\boxed{1000}$
↳ returned to A

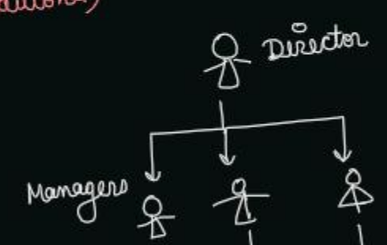
Use of Gas Limit ?
- hacker → started infinite loop() → Network is affected.
- ↳ After gas limit reaches → stop execution of transaction

$\boxed{\text{etherscan.io}}$ → demo of ethereum

Decentralized Autonomous Organization (DAOs)



(Traditional) **Normal organization**



→ Services offered are handled automatically
→ All activities are transparent & fully public

→ Requires human handling / centrally controlled automation
→ Activity is typically private & limited to public

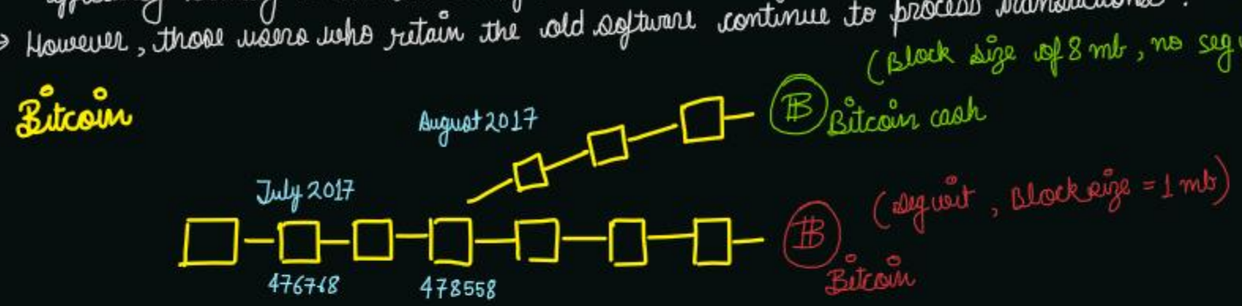
The DAO Stack

THE DAO

- organization based on DAO principles
- → smart contract

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 the transactions from older software, effectively creating a new branch of the blockchain.
→ However, those users who retain the old software continue to process transactions.



Soft Fork

→ Soft forks are a change to the protocol, but the end product remain unchanged.
→ A soft fork is a backward-compatible upgrade
  → upgraded nodes can still communicate with the non upgraded ones.
→ Old nodes can still validate blocks and transactions, but they just wouldn't understand them.
  → not upgraded nodes
  → upgrading didn't break rules!!

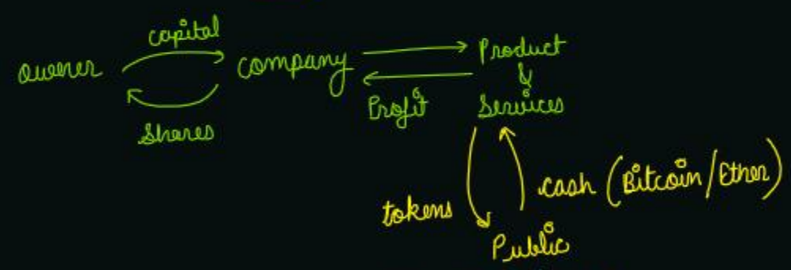
orphan block

(98% majority)

time → t1 t2 t3 t4 t5 because more ...

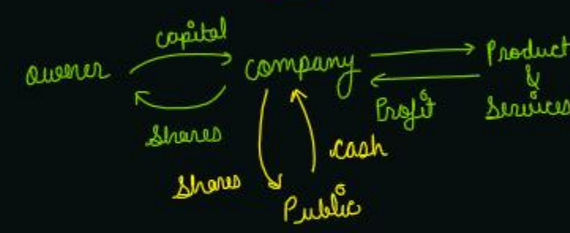
Initial Coin Offering (ICO)

ICO



→ no control / shares
→ no legal procedures

IPO



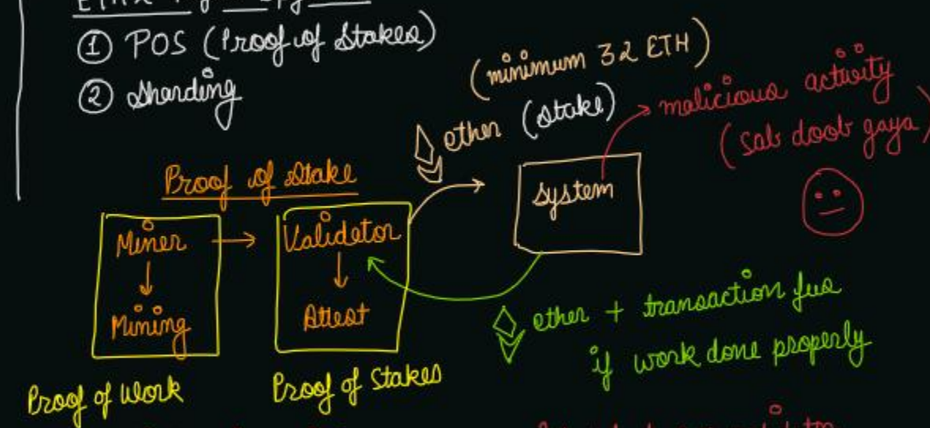
→ get control too
→ many legal procedures

Ethereum 2.0 / Serenity

1. Scalability
2. Security
3. Sustainability

ETH 2 Major Upgrades

1. POS (Proof of Stakes)
2. Sharding



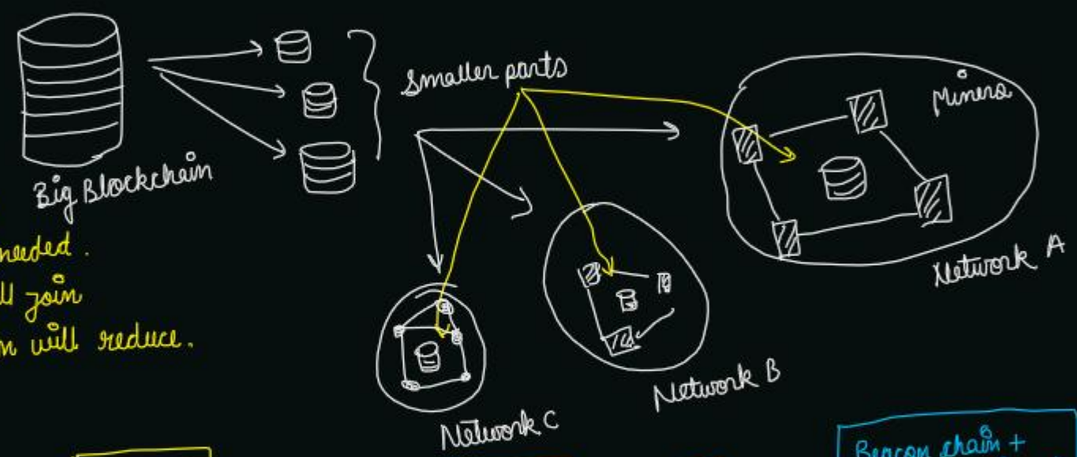
No competition like mining, system will select one validator

The more ethers you pay → more chance of getting randomly selected

Proof of Work (POW)	Proof of Stakes (POS)
→ Miners	→ Validators
→ High performance hardware required	→ mobiles / laptops are sufficient
→ Lots of electricity required	→ not much electricity required
→ More hashing power ⇒ more blocks	→ more ethers you put on stake ⇒ more blocks
→ 51% hashing power required to attack	→ 51% stakes required for attack
→ competition	→ no competition, random selection

Sharding

1. Transaction/second increases
2. Powerful & expensive computers aren't needed.
3. More validators will join
4. Energy consumption will reduce.



Beacon chain + Ethereum mainnet = Beacon chain + Ethereum mainnet + Shard chain ⇒ Beacon chain + Ethereum mainnet + Shard chain

Investopedia

Alt coins → {other than bitcoins}

1. Litecoin (LTC)
2. Theta (THETA)
3. Tether (USDT)
4. Cardano (ADA)
5. Chainlink (LINK)
6. Binance Coin (BNB)

→ New capabilities
→ consensus protocol {different}
→ 9000+ cryptocurrencies
→ largest market cap ⇒ altcoins Binance & Ethereum