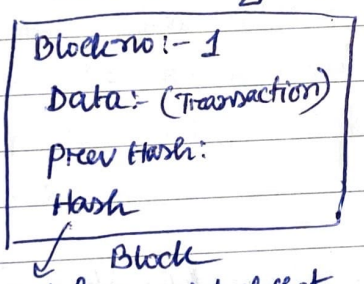
Blockchain

Blockchain: A disruptive technology, which has given us trust.
It is a dributed immutable ledger, which is completely transparent.
immutable ledger → once the data is feed to the block, it can not be changed.
Ledger → All the transaction are loaded here.
Distributed → The ledger is distributed in the whole chain.
Transparent → Everyone can see it.

Application of Blockchain:-
Product tracking, Smart contracts, Healthcare system, International mitee transfer.

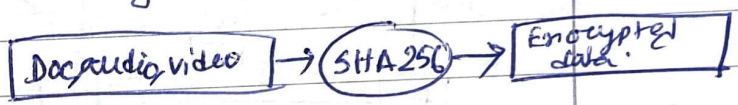
Smart contract → apply Ethereum blockchain.

Blockchain Hashing Algorithm:



Kind of fingerprint of that particular block.

Hash is generated by SHA256 algorithm.



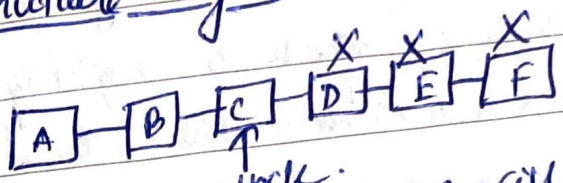
→ The encrypted data is 64 hexadecimal character. Each character is 4 bits.
So, total → 64×4 → 256 bits

The first block, which prev Hash: 00000.. is called Genesis block.

Five algorithm of Hash Algorithm

1. Oneway → The Hash value can not be traced back to PT
2. Deterministic → Same PT with generate same Hash value.
3. Fast computation.
4. Withstand collision → Hacker can not hack easily.
5. Avalanche effect → If any change in PT, Hash value will be changed

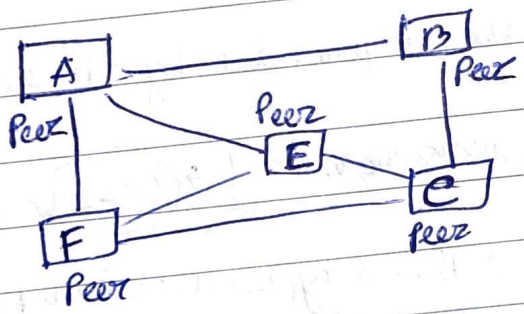
Immutable Ledger:



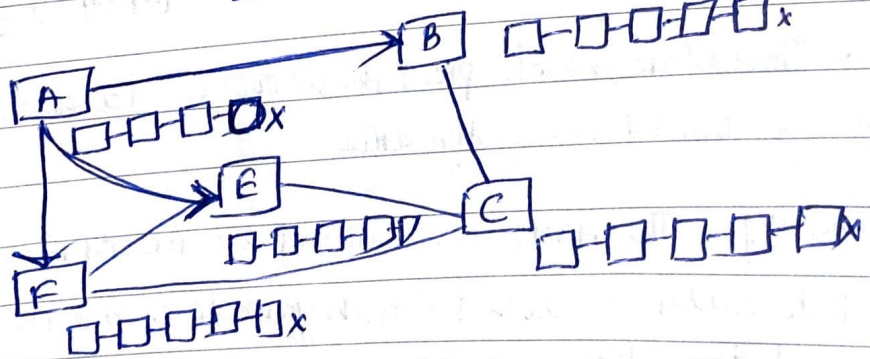
If any change in C, then D, E, F will be corrupted.

Immutable ledger meaning, if attacker attack any one single block then all the followed blocks will be changed, as a result all the blocks in the the blockchain will be notified and all compiter will work together to get back the oreginal data of the attacked block.

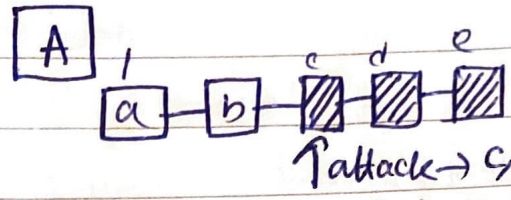
Distributed P2P N/w:- (where the whole data is not present to a particular server instead it is distributed in there peers.



A-E → Miners, every miner has a chain of block.



If Miner A, mines a new block in his chain, then he sends that information to his peer node/miners → B, E, F. once, the transaction is verified then B, F, E also add the block in their blockchain. And the C will also add.



Suppose, hacker hacked all the blocks after c as well. then, this chain of block will be compared to the peer miners to check of blocks, if its not same, then miner A will change his block to original block.

It is difficult are rather impossible to hack blockchain because of its immutibity and P2P n/w.

Blockchain Miners:-

Transaction will go to the memempool. then Miners try to add that transaction to their block by solving a complex mathematical Problem. Miner solve the problem first and create a block for themselves.

Transaction → Solve mathematical Problem → Create the block by Miner who solve the problem first → other group of Miner will verify the transaction → Then they will add the block to their chain

Miner will get reward.

Byzantine Generals Problem:- (nodes → systems)

Solⁿ has given by Miguel Castro, where one node could have been an attacker.

The recovery mechanism allows the algorithm to tolerate any number of faults over the lifetime of the system provided fewer than 1/3 of the replicas become faulty within a small window of vulnerability.

→ meaning the mechanism will follow the majority decision.

Consensus Protocol

types:-

Proof of work (POW) :→ Bitcoin
Proof of Stake (POS) :→ Ethereum

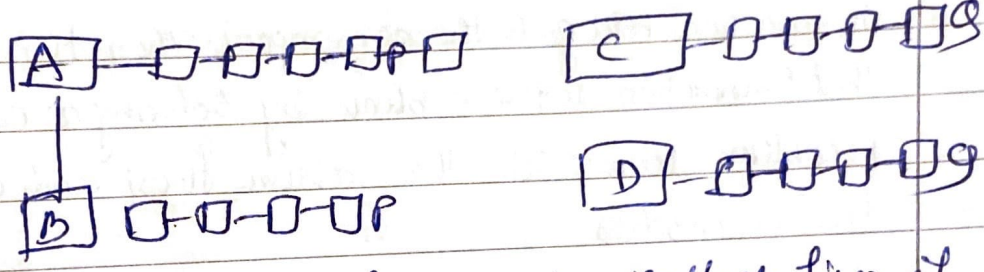
Miners gets reward for adding block and also transaction fee.

→ Consensus protocol check if the transaction is valid or not and Prevent contrasted attacks

→ Competing chain problem :-

Longest chain rule :-

Suppose two miners create the block at the same time and ask their peer nodes also, ~~Go~~ the peer node add it



But for the next block whoever mine the block first if here, A mine first block then p will be added to all A, B, C, D.
But q will be discarded from the block chain.

Module-B

Cryptocurrency :

Bitcoin is the first crypto-currency e invented by Satoshi Nakamoto.

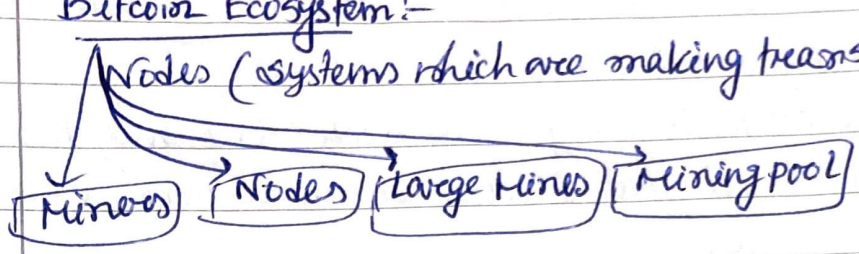
Technology → Blockchain
Protocol/coin → Bitcoin, Ethereum, Waves
Token →

TRX | SNT
REP | AE

WGTB | DI
JNTL | HGR

Foundation: Founder of Bitcoin → Satoshi Nakamoto invented in 2008.

Bitcoin Ecosystem:-



Bitcoin's Monetary policy:-

Monetary policy → Supply of money maintaining

The Halving:- (total bitcoin can be produced is 21 million) → Supply Cap

Event	Date	Block Number	Reward
Launch of Bitcoin	3 Jan, 2009	0	50 new XBT
1st halving	28 NOV, 2012	210,000	25 new XBT
2nd halving	9 Jul, 2016	420,000	12.5 "
3rd halving	11 May, 2020	630,000	6.25 "
4th halving	Expected 2024	740,000	3.125 "
5th halving	" 2028	850,000	1.5625 "
Max supply reached	Expected 2140	6,930,000	0 new XBT

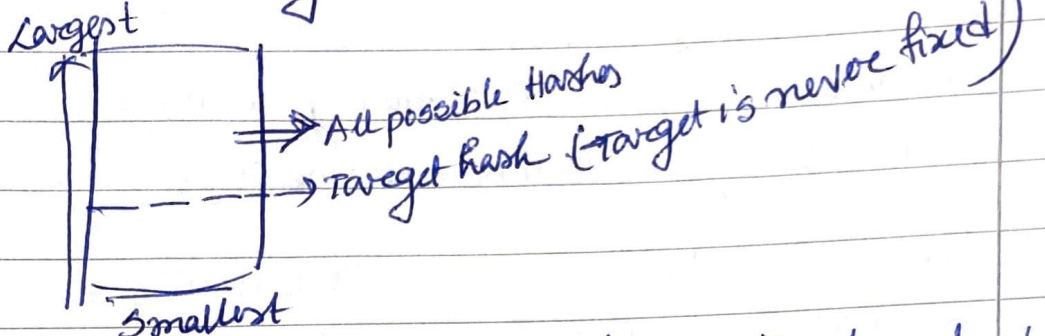
Block Frequency: This states that on an average it will take 10 minut to create a new block.

Nonce: → Miner solve a complex mathematical eqn, i.e. Nonce.

Miners get a target hash value, by changing the Nonce value miners try to generate the hash value, if the generated hash is less than the target value then, only the block will be created.

Nonce: The nonce is the number that blockchain miners are solving for

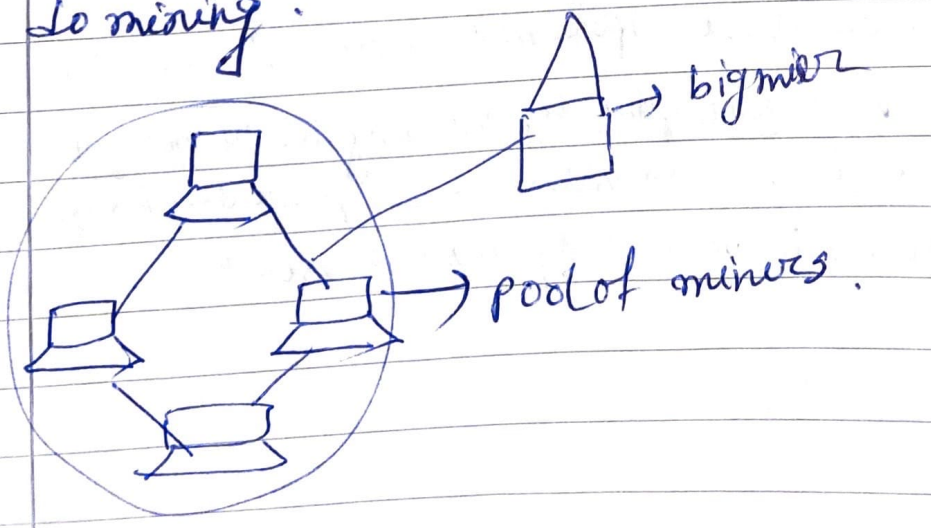
Target:- 1) Target is a number used in mining.
2) It is a number that a block hash must be below for the block to be added on to the blockchain.
3) The target adjusts every 2016 blocks (roughly two weeks) to try and ensure that blocks are mine once every 10 mints on average.



If any N/W started mining very fast then the target value is set to different and difficulty level get increased.

Mining pool:

The Problem arise when, only the big miners who have more hashing skills do the maximum hashing as a result small miners could not get a chance. So, to avoid this small miner get together with other nodes/system to create a pool of networks. where few miners work together to solve the target hash and do mining.



The reward is decided depending on the miner's hashing power.

→ The miners which are a part of the mining pool, take different range of Nonce value to get the target hash value.

Different mining pool → F2Pool, Poolin, ViaBTC etc.
all have different hash rate.

~~**~~ reward is also decided based on the hash power of miner in which network pool that miner belongs to.

CPUs Vs GPUs Vs ASIC

CPU → 10 MH/sec → Generate Hash value 10 mega Hashes/sec
GPU → 1GH/sec 1 giga hashes/sec
ASIC → 1000 GH/sec 1000 Giga hashes/sec

Came in 2013,

Now, ASIC can generate almost 10 Trillion hashes per sec.

Nonce Range:-

Nonce is a 32 bit number. (Range of Nonce = 0 to $2^{32}-1$) $\simeq$ 0 to 4×10^9

Total number of possible hashes = XXX ···· 64bit
(0–15) → 16

$16^{64} \simeq 10^{77}$

As, $10^{77} >>> 4 \times 10^9$ → so we do not have enough nonce to generate all hash.

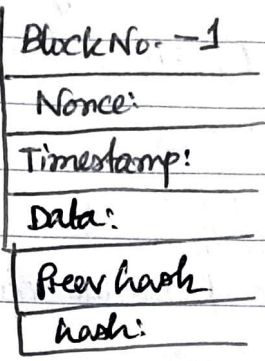
Timestamp: Time stamp is a number which gets changed in every second. So, the hash value also gets changed.

4 billion nonce get exhaust in 40 sec only.

0.1 billion " " " 1 sec only.

→

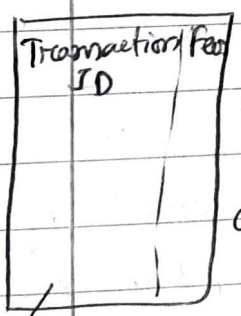
Timestamp



So, when the timestamp gets changed in every second the hash value also gets changed. and the Nonce can be checked utilize again.
So, because the timestamp is getting change the total Nonce will not be used and exhaust.

**** Current hashing rate is equal to 150 million trillion hashes/sec.
↳ So, 4×10^9 nonce will be covered in $= (4\times10^9)(10^6\times10^{12})$
$= 4\times10^{-9}$ sec <<<< 1 sec.

Mempool:



Thousands of transaction

So, when the nonce value get exhausted in below 1 sec, then miners started adding transaction in their block.
Miners change the lowest fees transaction with some one lowest fees transaction from mempool.
So, hash value gets changed and start utilizing the Nonce.

So, using mempool miner can change their transaction and use the nonce value again and again.

How do Mempool work?

→ Mempool is not a centralized system. Every person and system node, (who currently not mining) have a mempool. All the transaction first goes to the Mempool and then miners picks the transaction from there. Once Miner picks the transaction from mempool the transaction gets added to the miners block and similarly all the other nodes as well and that transaction gets removed from the mempool.

Transaction and UTXOs :-

A → Me 0.4BTC
B → Me 0.3BTC
C → Me 0.2BTC
~~D → Me 0.8BTC~~ ← 0.2 → Me

→ UTXOs (unspend Transaction outputs)

for cryptowallet, If we want to spend 0.5 BTC, then we have to choose a previous transaction which is greater than 0.5BTC. and then we will spend that and between value will come back to me.

0.8 BTC from D → 0.5 for coffee
→ 0.2 back to me.

So, once spend then 0.8BTC will be extracted from my UTXOs and 0.2 will be there. And 0.5 BTC will be then added to Coffee shop UTXOs.

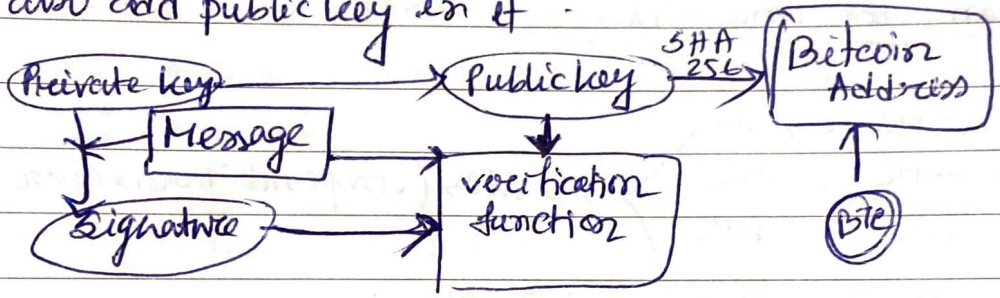
Transaction fee :-

When you give any transaction to Miners or Miners take your transaction from mempool and add that to their block, you have to give a particular transaction fees to the Miners. If your transaction fee is very minimum then sometimes miners does not pick the transaction.

Cryptocurrency Wallets:-

Wallets add all those transaction which are not ~~added~~ used and then add that.

When the wallet is ~~gone~~ generated, then we generate a private key and from the private key we generate public key.
the signature is used the private key + Message.
then we put the Msg and Sign to a verification function and also add public key in it.



Segregated witness :-

If the size of the block gets increase, it will take ~~more~~ more bandwidth
It means that the signature and public key send separately, from the block.
As it is taking maximum space.

If we segregate those, then we can add more transaction in the block.

- Public key generally used to send a transaction.
- Bitcoin address is generated from public key.
- Bitcoin address is used to receive a transaction. i.e, when someone send bitcoin we give them the bitcoin address.

*** Bitcoin address is basically worked as an extra layer to protect your private key. So that the ~~hacker~~ hacker can never get discover the private key.

HD wallets (Hierarchically Deterministic wallets):-

It is used for privacy issue, so that the hacker can not recognise any sending/receiving transaction pattern.

Master ~~private~~ generate many private key an keep a ~~Public~~ key

Private

Check on master ~~public~~ private key