Blockchain :- Distributed Ledger

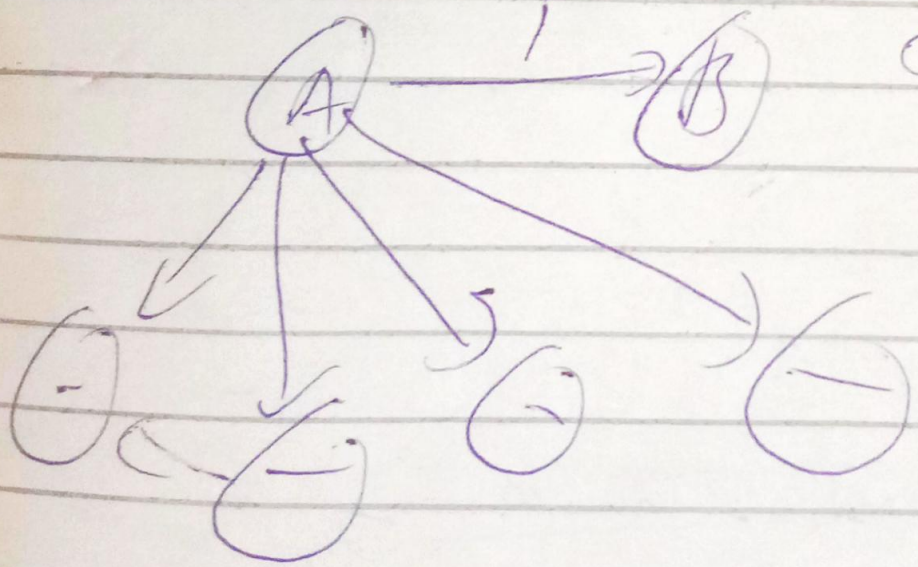
Node & block are different terminologies

↓

physical entities
physical etc

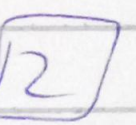
Broadcasted data after transaction

for consensus
verification from
other nodes



1

verified
new added
block



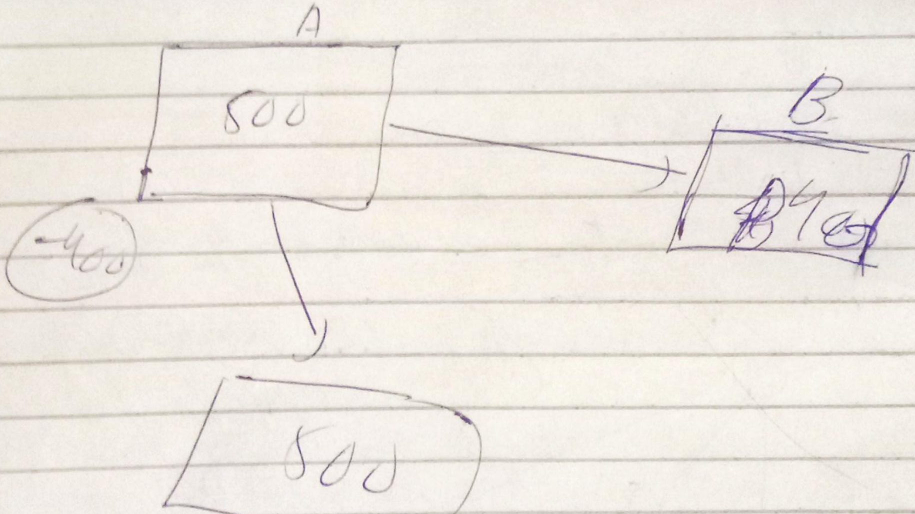
Genesis block Research

Merkel Tree: It generates hash for every block

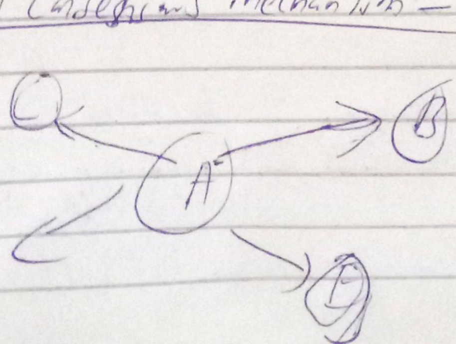
hash is freely available on blockchain whilst data is encrypted

Data encrypted form mein cledha pra hota hai or us ke hashes cledha pe hote hain

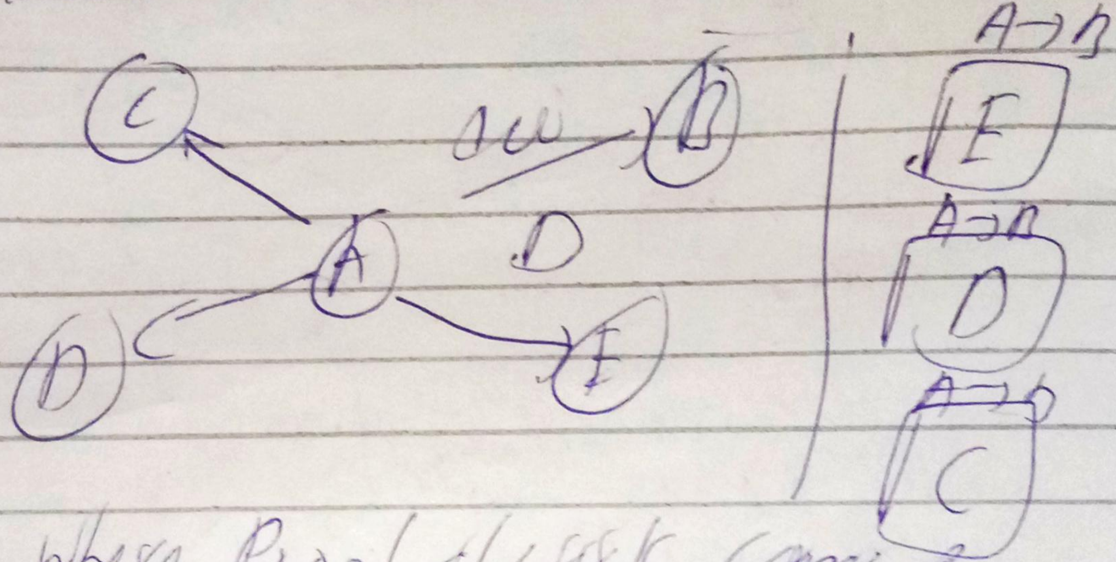
Double Spending: When transaction takes time to deliver & you make more transactions until the value updates.



Need of Consensus Mechanism —



If Alex say a transaction create 3 blocks at the same time



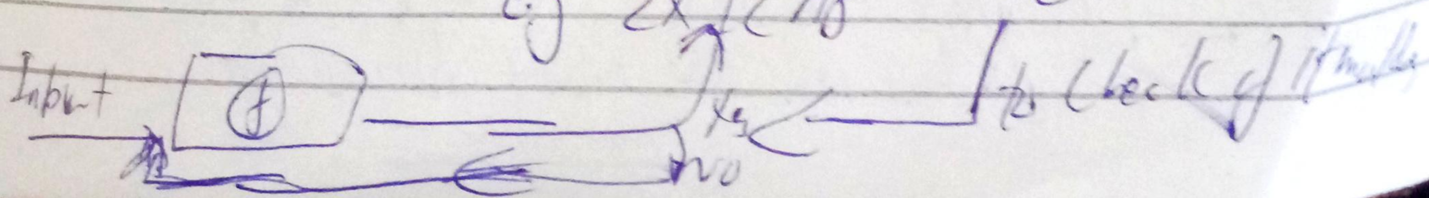
This is where Proof of work comes in to mitigate this issue as there shall be only 1 transaction for the creation of a block

Proof of work:-

> You do something
> You do random guesses
> You do mathematical computations

Nonce: Number used once
e.g 2X, 3, 45

HAC find method



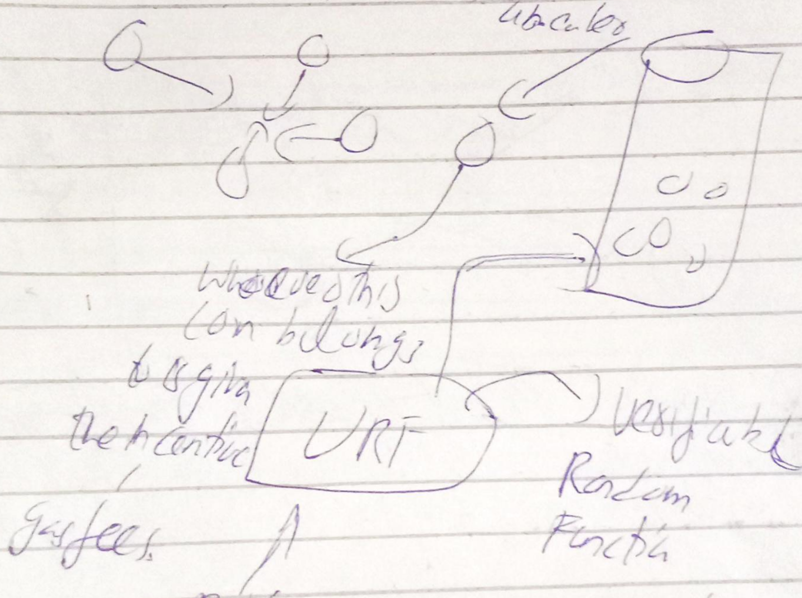
If correctly gotten, you got gas fees.

Proof of work requires gpu (physical Resources) to mine

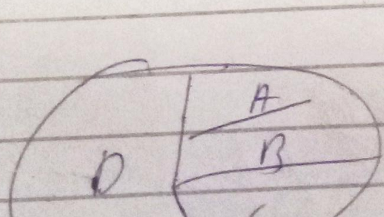
Proof of Stakes:-

> Do not require any physical hardware

Persons put their coin in



Picks a random coin from the banker

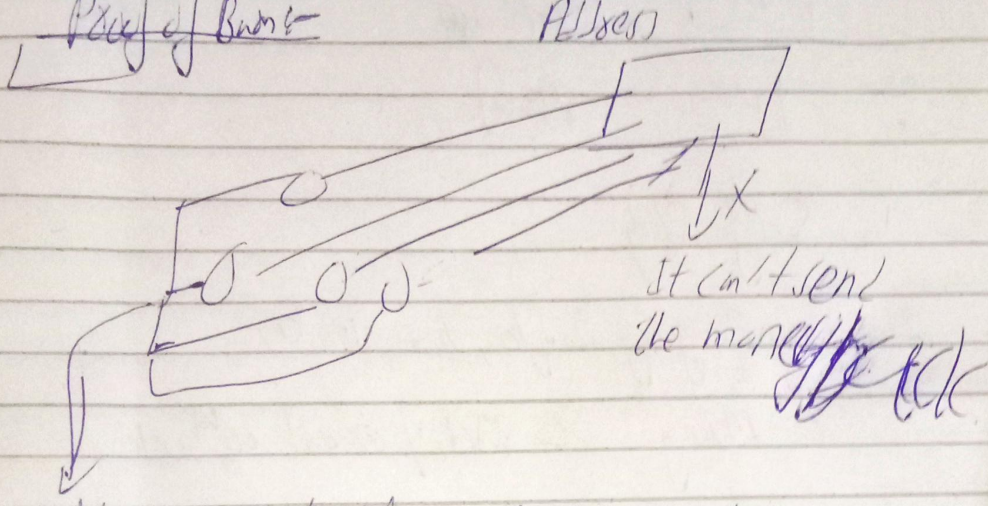


D has the most stake in the pie & thus has the most privileges

What happens to the rest of the people who don't get at 51 the bar.

Full Nodes ??

VRF doesn't have a hashing function



All of these people send their amount

If we are not mining then what does mining mean??

Again Proof of Transfer:-

Stacks

C++

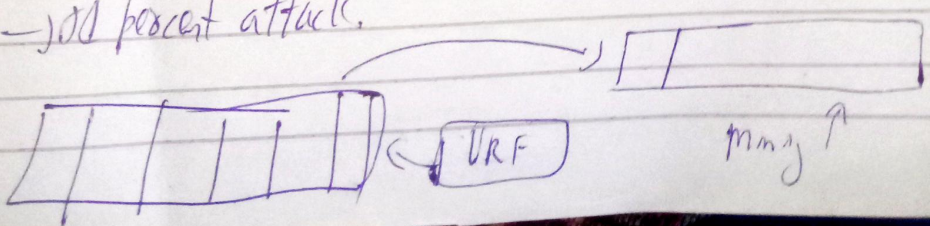
→ Secure

→ C++, mature

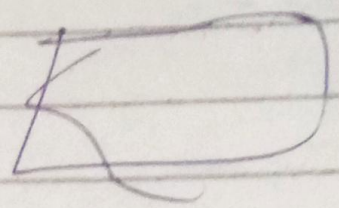
→ 100 percent attack.

Satoshi Version

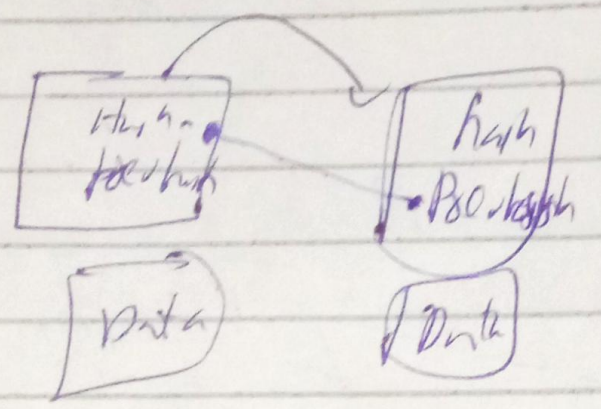
Github



Now stacks uses Proof of Transfer



so that we don't safely rely on bitcoin ledger.



Self Stg

→ Proof of transfer, burn, stake

→ Mining → 51 percent attack

→ Full Nodes