Once the CPU effort has been expended to make it satisfy the proof of work, the block cannot be changed without redoing the work.

→ you cannot have a single person determining everything

→ PoW is essentially one-CPU-one-vote

→ majority decision by the bigger chain

Network → steps

① new transaction broadcasts to all nodes

② Each node collects transactions into a block

③ Each node works on finding a difficult pow for its block

④ When a node finds a pow, it broadcasts the block to all nodes

⑤ Nodes accept the block only if all transactions in it are valid and not already spent.

⑥ Nodes express their acceptance of the block by working on creating the next block in the chain, using the hash of the accepted block as the previous hash.

Incentive → for finding pow you get reward.

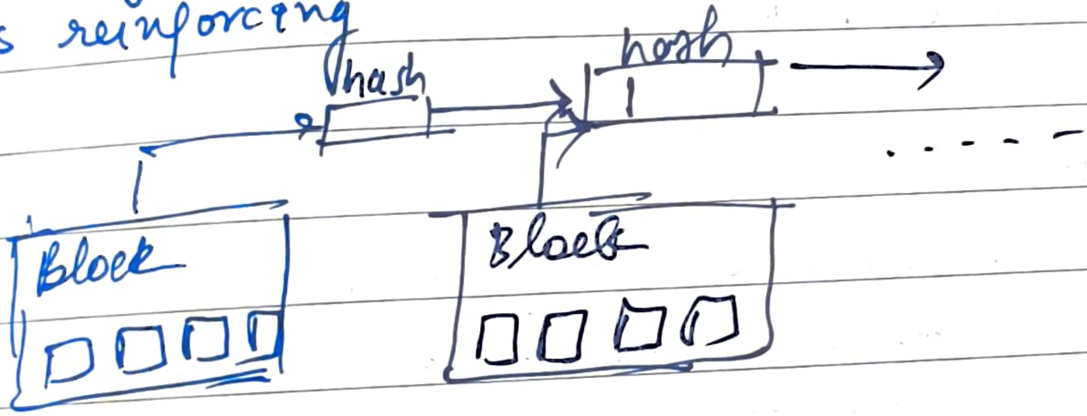
The incentive may help encourage nodes to stay honest.

Timestamp

→ better world is ordered server
↳ every blocks hash, depends on previous block's hash

→ timestamp server

→ timestamp proves that the data must have existed at the time, obviously in order to get hash
→ Each timestamp includes previous ts in its hash forming a chain with each additional ts reinforcing



Proof-of-work

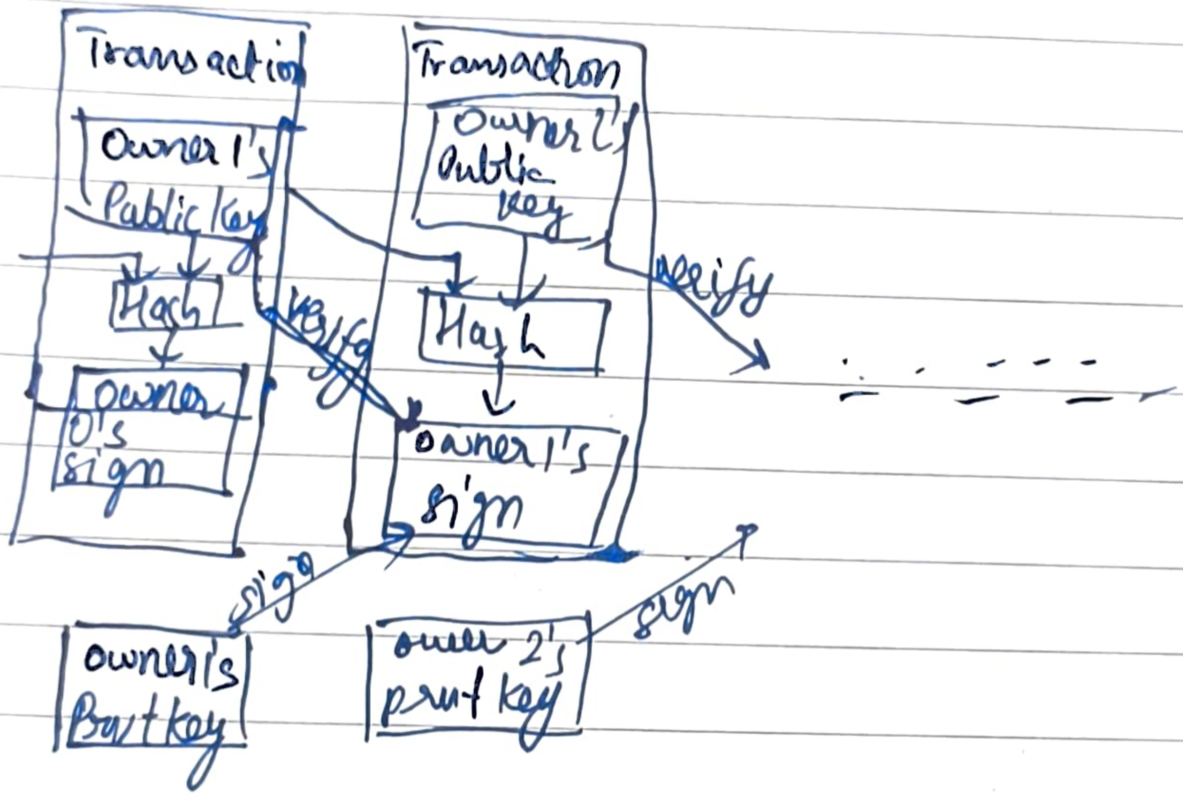
↳ to implement a distributed ts server on a p-2-p basis. → based on Adam Back's hashcash created for Denial-of-service attack.

Thee avg work required is exponential in the no. of zero bits required and can be verified by executing a single hash.

→ Trying to find the zeros is very hard.

Transactions

we define an electronic coin as a chain of digital signatures

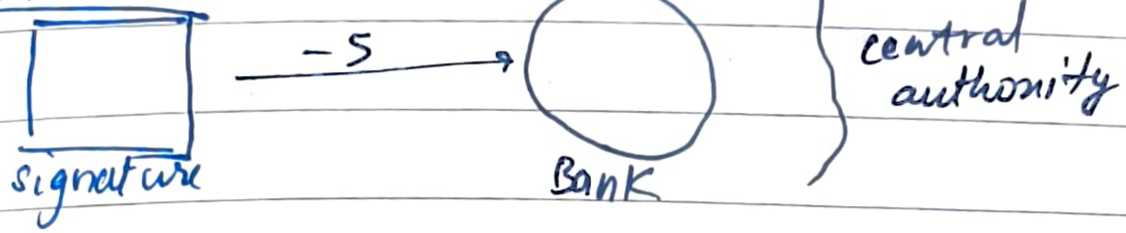


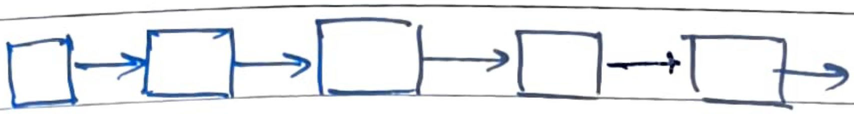
→ Banks usually don't use private key

→ The only way to confirm the absence of a transaction is to be aware of all the transactions.

"Bitcoin: A Peer to Peer Electronic Cash System"

Introduction





work over here means → mining to find the nonce.

⇒ even if you break the chain, you won't have enough compute power or proof of work.

⇒ messages are broadcast on a best effort basis

⇒ centralized problem → Completely non- irreversible ~~for~~ payments is not really possible → cost of mediation increases transaction costs limiting the minimal practical transaction

⇒ Bitcoin makes every transaction irreversible, removing the risk of a fraud.