BitCoin

↑

Digital Currency

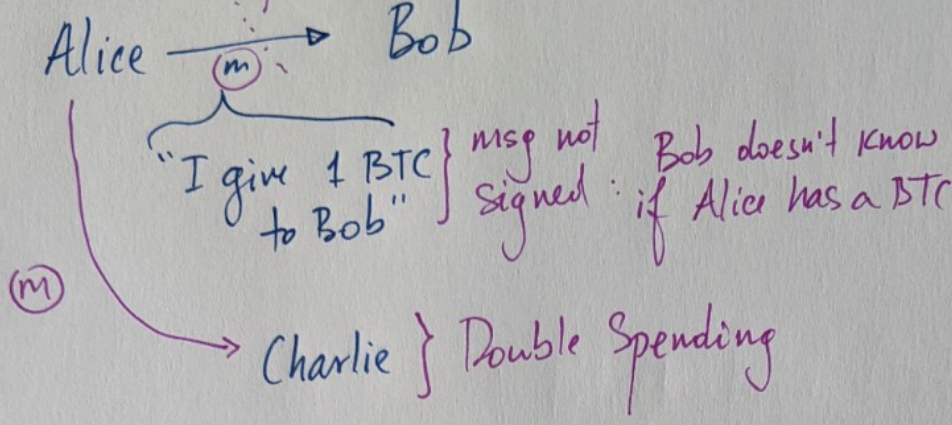
Alternatives
Smart Contracts

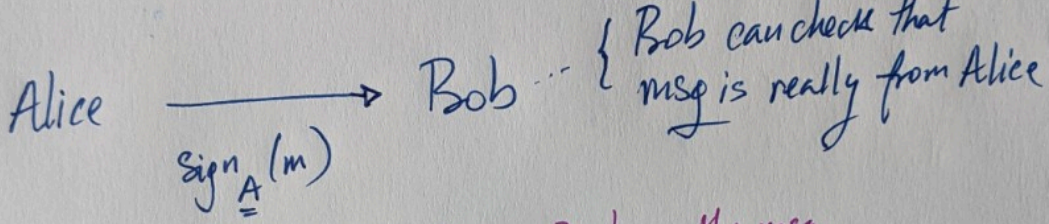
Key ideas : Concepts

+ Proof of Work (PoW) ... Alternatives Proof of stake (PoS)
  ⇒ Cryptopuzzle — originally invented for SPAM email
+ BlockChain (Dist. Ledger)
  ⇒ Ordering on operations (txns)
  Read/Write shared State
+ P2P + Byzantine threat model ... Alternatives Private BChains (not open)
  Arbitrary peer Behavior
+ Eventually Consistency ?
  If you wait long enough then everyone will observe same state

Blockchain

Intercepted : Man in the middle





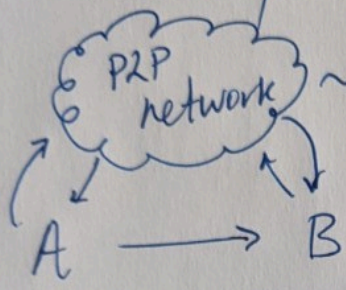
× MIM : at most can Replay the msg

× Double Spending still a problem

Bank ⟹ Distributed P2P Context

"Make everyone the Bank" ⟹ Bank is public / transparent

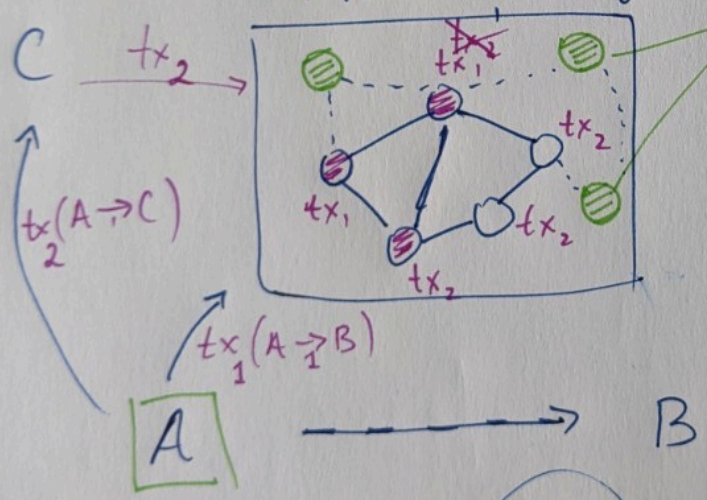
⇒ all peers in the system track the ledger of txns



× double spending
× Concurrency
] PoW + Blockchain

× Incentives] Reward P2P peers

× Trust] Assumptions about majority of non-malicious CPU power



"txn committed" if majority of P2P netw. know about it

Any two majorities overlap

Requires to know the # of nodes in system

⇒ Easy to Join

⇓

Easy to create "Sybils" by 1 person

⇒ Sybil Attack

Proof of Work (PoW)

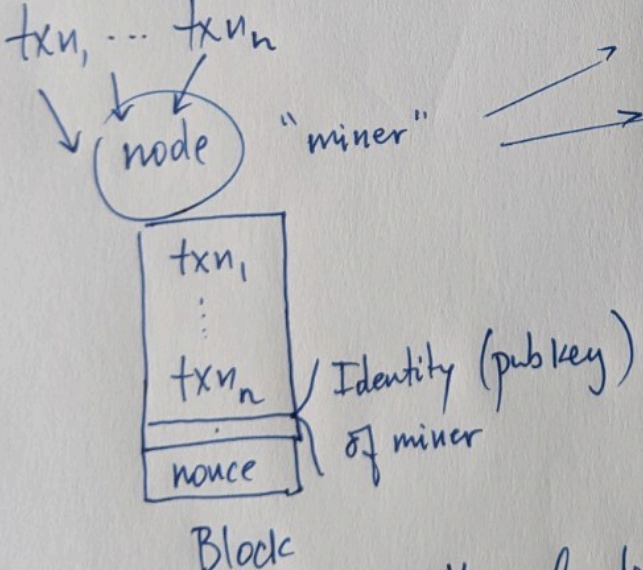
(1) Make validation of txns in the network "difficult" (Why? A: Sybils)

⇒ You need real physical resources (CPU cycles for computing PoW)

(2) Incentives for nodes to compute PoW

- Reward for solving a PoW ⇒ # of BTC
- Scales with amount of CPU cycles

(3) Transactions come with a fee that is given to a node that "validates" it using PoW



(M1) Check txn_i valid (consistency check)

(M2) Solve a cryptopuzzle (PoW)

h = sha-256 hashing fn.

Find a nonce value s.t.

h(Block) ≤ target value

i.e., h(Block) = 0x00...00 5AF42...

Difficulty for PoW task = # of leading zeroes

Key Conditions for PoW

1. Difficult to find nonce
2. Easy to verify (check) the nonce

Mining generates reward to miner (in BTC form)

⇒ Race between miners to mine blocks ⇒ Mining pools for cooperation

(Miners have to balance # of txns in a block with the fact that other Miners are already mining) — Select some # of txns (Bound on block size)

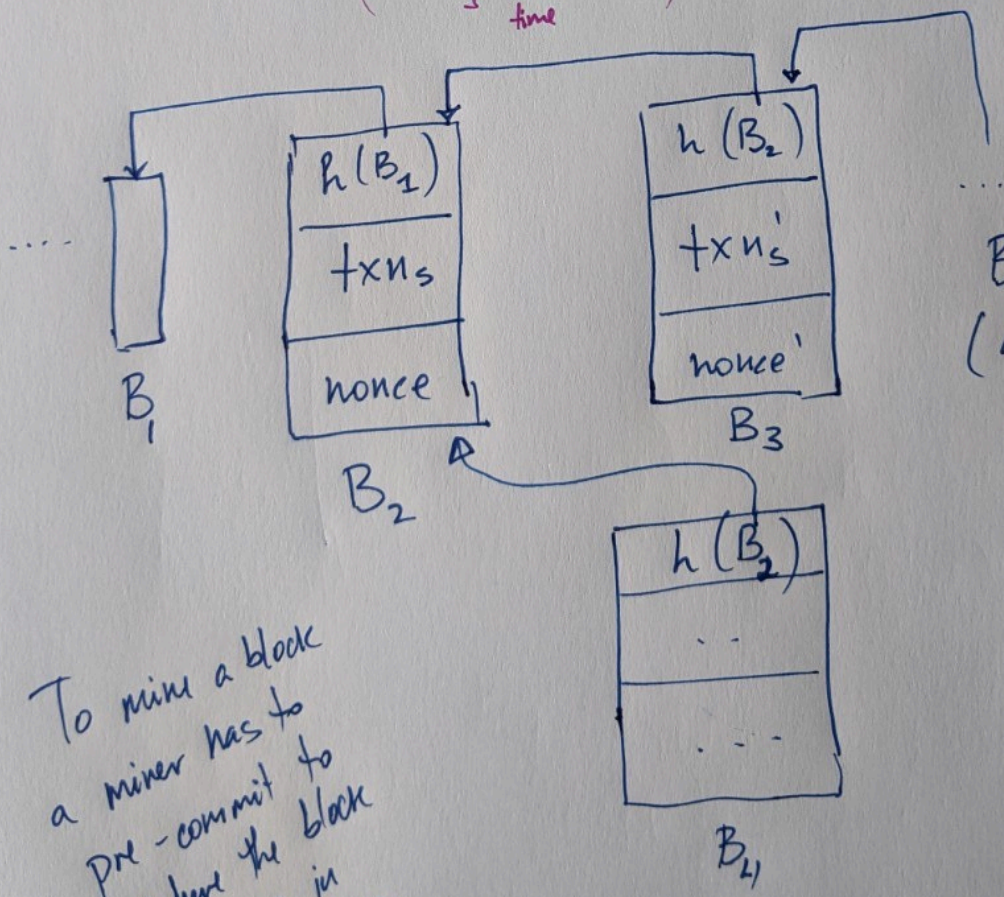
BTC mining reward is generated until ~ 2140

↓

After 2140 Mining is incentivized using only txn fees

Missing: Ordering of txns

$(txn_1 \overset{\text{time}}{\leq} txn_2)$



To mine a block a miner has to pre-commit to where the block will go in Blockchain

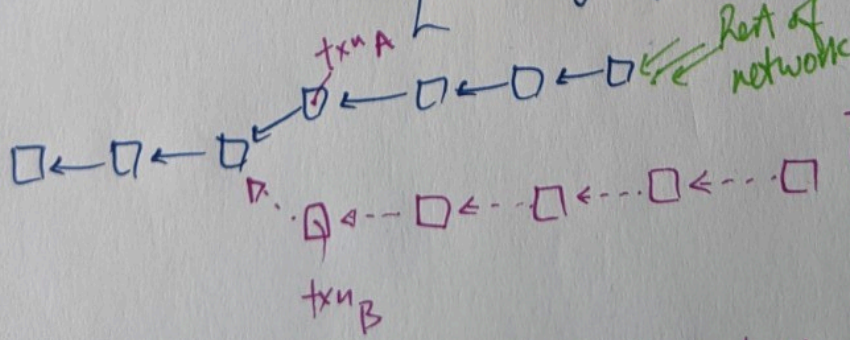
Miners — Work along the longest chain (that they know)
— Keep track of all forks (the entire tree)

In short term "longest chain" is unclear
- Race cond. in mining
- Network latency
- Network connectivity

But... in long term "longest chain" is stable

⇒ txn is not "confirmed" Unless
1. txn is on longest chain } Essential for total order
2. Must have 5 blocks that follow it } heuristic
"6 confirmations"

Implications:
1. Blocks are immutable: "ledger" → Append Only
2. Difficult to create a fork + Convince network to follow it
→ Requires maj. of CPU power



txn_A & txn_B conflict: "double spend"

BitCoin Overview

1. Flooding Txns
2. Mining process to = 1. Validate txns, 2. Generate blocks
3. Flooding Blocks (that include txns)