pg 1

BitCoin

↑

Digital Currency

Alternatives
Smart Contracts

Key ideas: Concepts

+ Proof of Work (PoW)
  ⇒ Cryptopuzzle — originally invented for SPAM email

Alternatives
Proof of stake (PoS)

+ BlockChain (Dist. Ledger)
  ⇒ Ordering on operations (txns)

Read/Write
shared State

Alternatives
Private BChains
(not open)

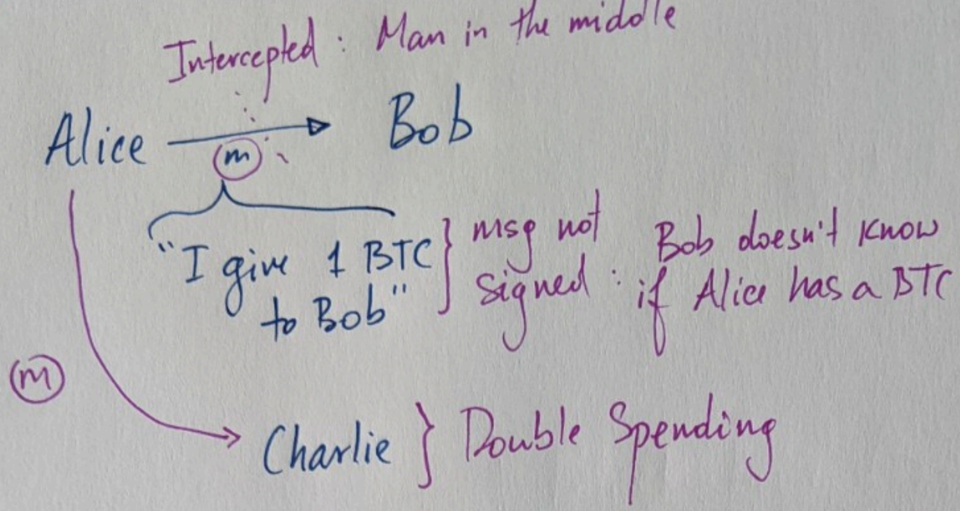
+ P2P + Byzantine threat model

Arbitrary peer
Behavior

+ Eventually Consistency ?

If you wait long enough
then everyone will observe same state

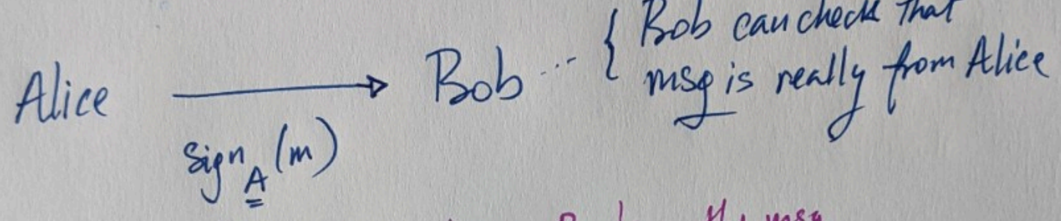
Blockchain



msg not signed : Bob doesn't know if Alice has a BTC

Charlie } Double Spending

⇓

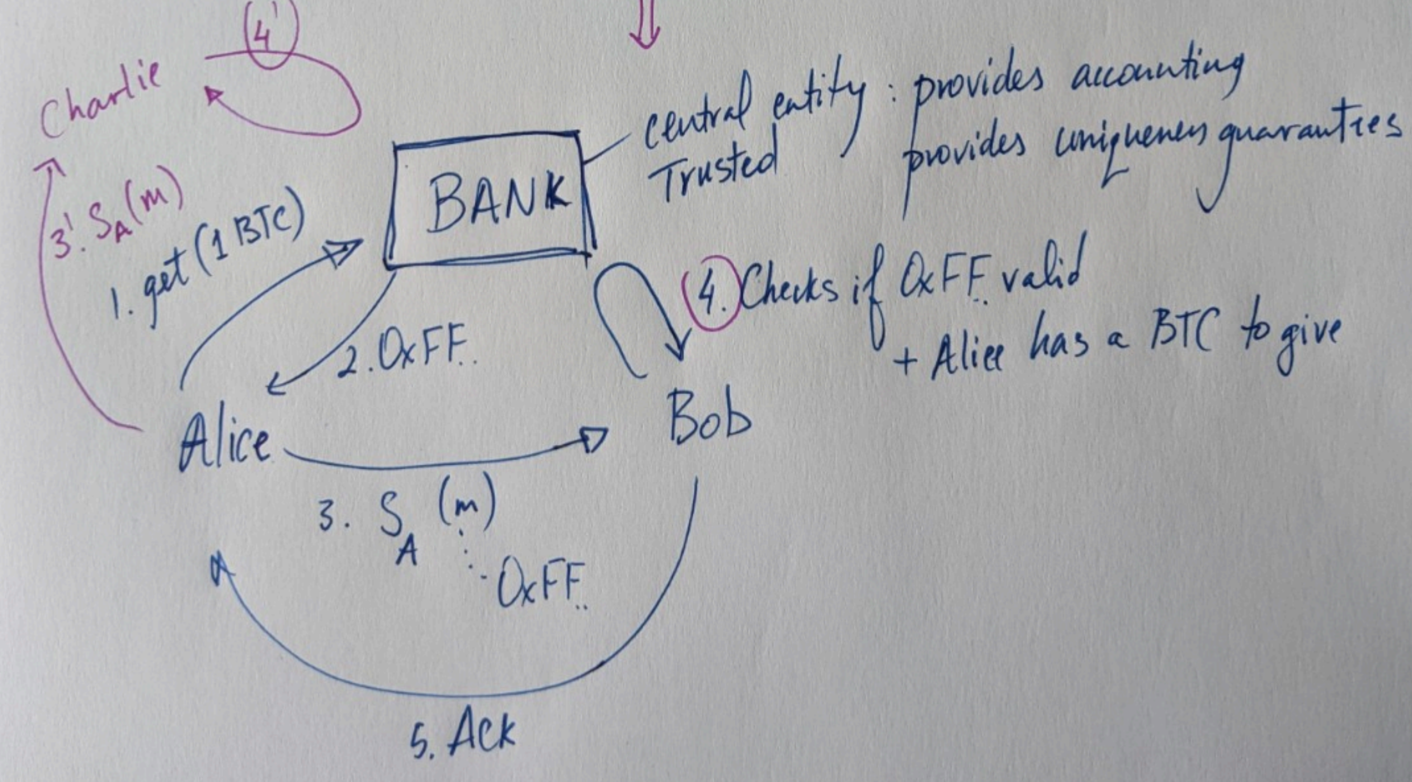


Bob can check that msg is really from Alice

× MIM : at most can Replay the msg

× Double Spending still a problem

⇓



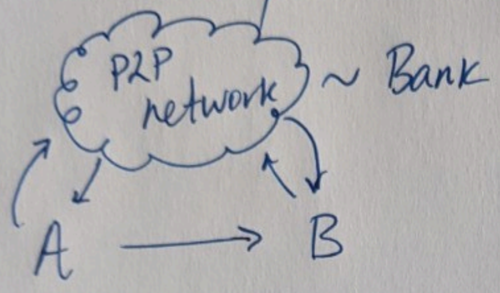
central entity
Trusted : provides accounting
provides uniqueness guaranties

4. Checks if 0xFF.. valid
+ Alice has a BTC to give

Bank ⇒ Distributed P2P Context

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

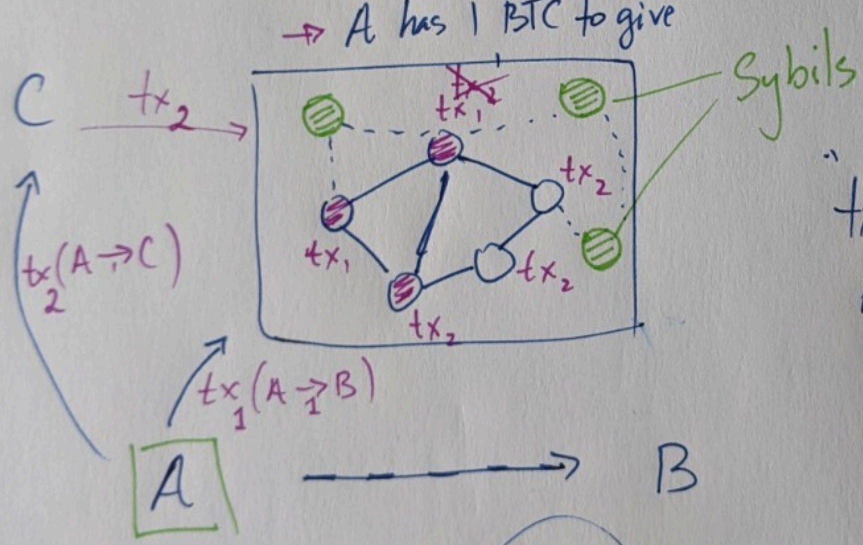
⇒ all peers in the system track the ledger of txns



× double spending] PoW + Blockchain
× Concurrency]

× Incentives] Reward P2P peers

× Trust] Assumptions about majority of nodes non-malicious



"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)

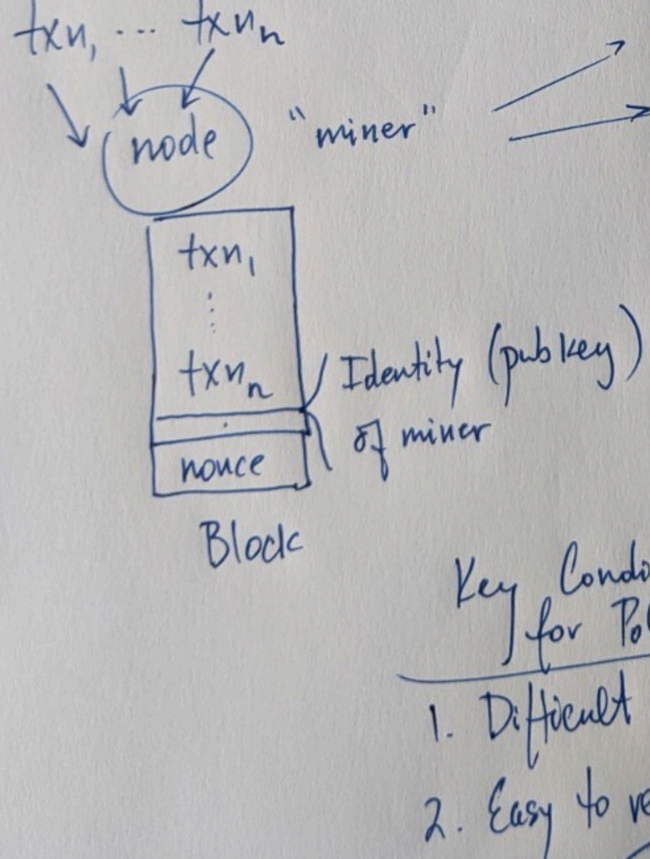
⇒ You need real physical resources (CPU cycles for computing PoW)

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.

$h(\text{Block}) \le$ target value

i.e., $h(\text{Block}) = \underbrace{0x00\ldots00}_{\substack{\text{Difficulty for PoW task}\\ \text{\# of leading zeroes}}}5AF42\ldots$

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)

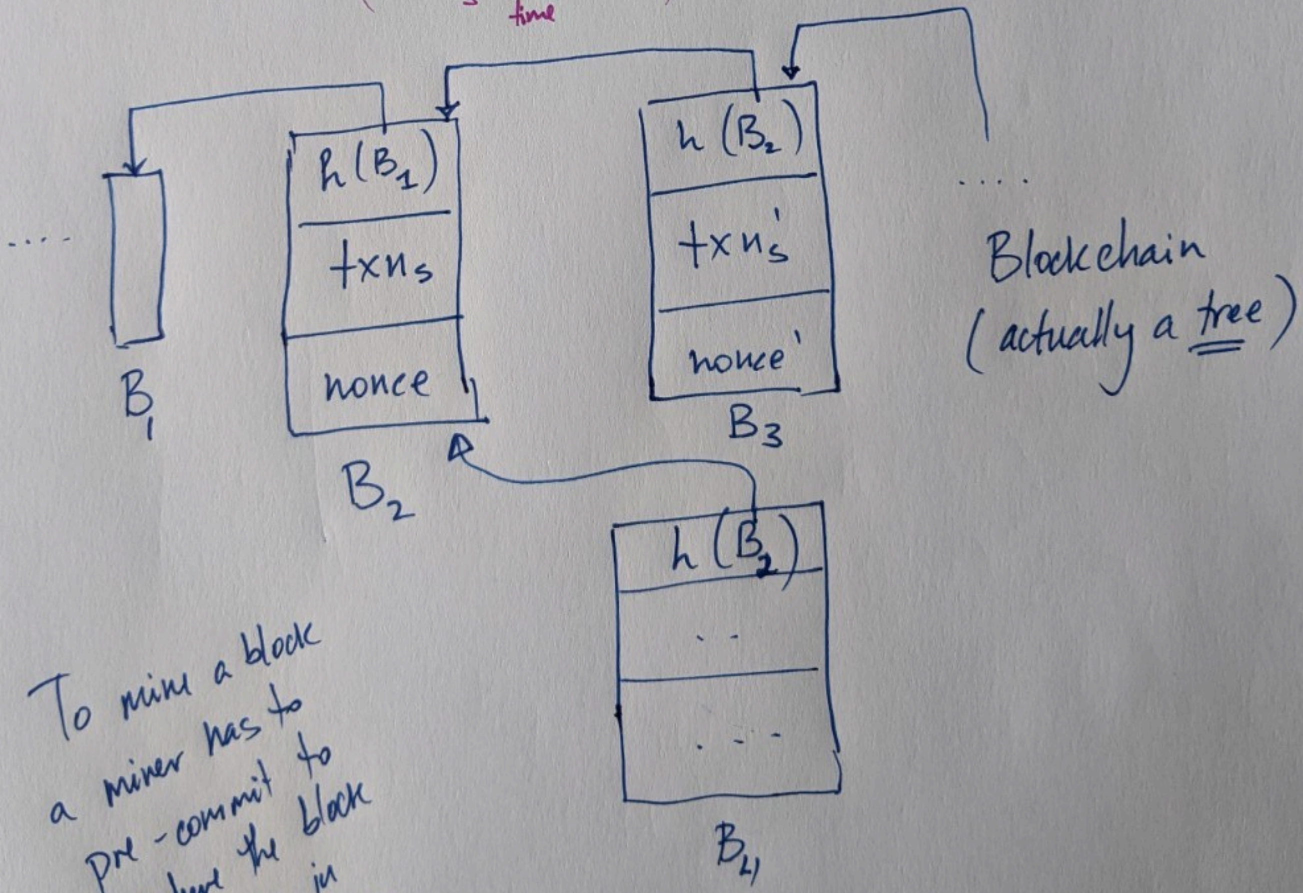
BTC mining reward is generated until ~ 2140

↓

After 2140 Mining is incentivized using only txn fees

Missing: Ordering of txns

$(txn_1 \underset{time}{\leq} txn_2)$



Blockchain (actually a tree)

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

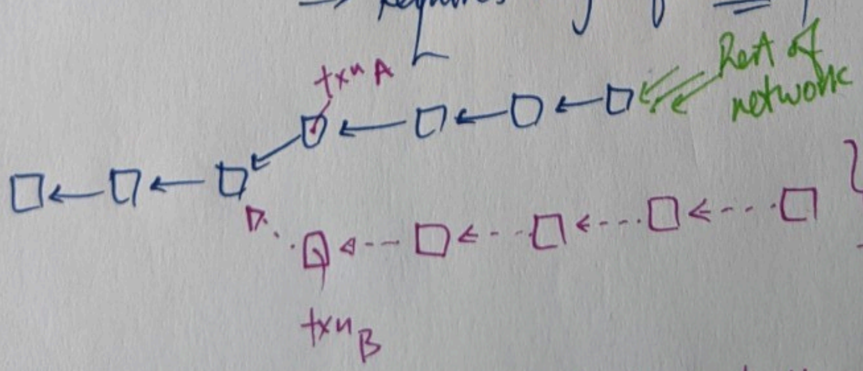
Miners — Work along the longest Chain (that they know)
— Keep track of all forks (the entire tree)

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



} Need to Mine a longer chain than network

txn$_A$; txn$_B$ confict : "double spend"

BitCoin Overview

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

The End