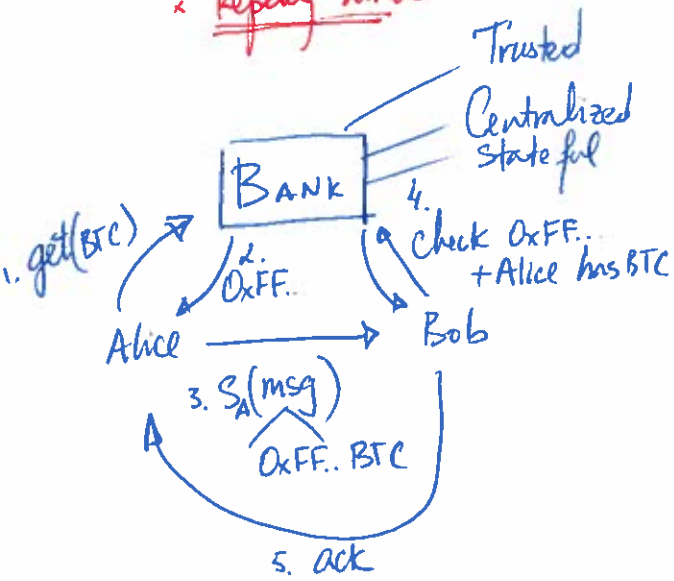
BitCoin:

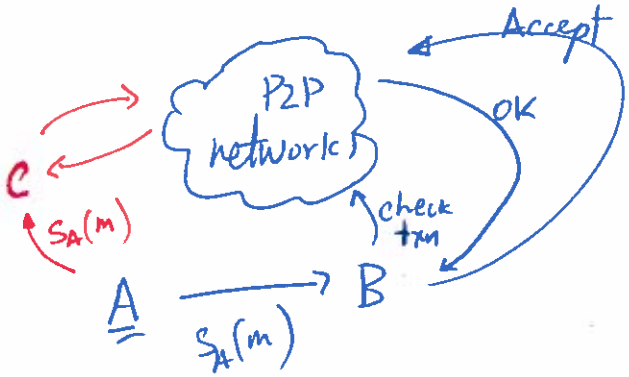
Key ideas:
+ proof of work
+ blockchain (Distributed ledger)
+ P2P + byzantine context.
+ Eventual Consistency

(A) Alice → Bob : m = "Tim giving Bob 1 BTC" — msg not signed
MinM
m → Charlie } Double spending

(B) Alice → Bob (verify msg from Alice)
MinM
sign$_A$(m)
× double spending
× Replay attack

(C)


(D) Have everyone keep track of who owns which BTC
i.e., shared ledger with all txns
public
BlockChain



× double spending
× concurrency
× incentives
× trust
] PoW + Blockchain
] Reward
] majority non-malicious

⇓

problem to solve is sybils

BitCoin ~ P2P Bank
= "Make everyone the Bank"
Replicated Bank State

Proof of Work (PoW)

① Make validation of txns computationally difficult

② Incentives for nodes to perform PoW

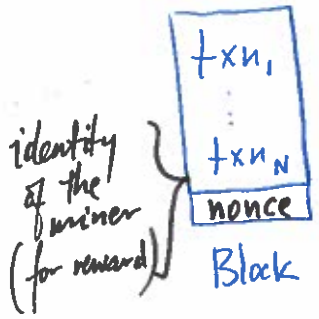
- virtual nodes → defer "Sybil" attacks
- to validate a node needs phys. compute
  - ⇓
  - (#) Challenging to have a legitimate node
- Spam is hard
  - ⊕ transactions have a cost

[Proof of Stake alternative to PoW]

- Need resources to truly join network : Raise bar for participation (compute)
- txn processing is slow

txn1 ... txn n

node ~ miner



(1) Check txn_i valid (txn_i passes consistency checks)

(2) Solve a cryptopuzzle (PoW)

h = sha-256 hashing fn

Find nonce s.t. $h(\text{Block}) \leq \text{target}$

or, think about target as # of leading zeroes

i.e., $h(\text{Block}) = 0x\underbrace{00\ldots00}_{\text{target \# of 0s} \sim \text{"Difficulty"}}3aF42\ldots$

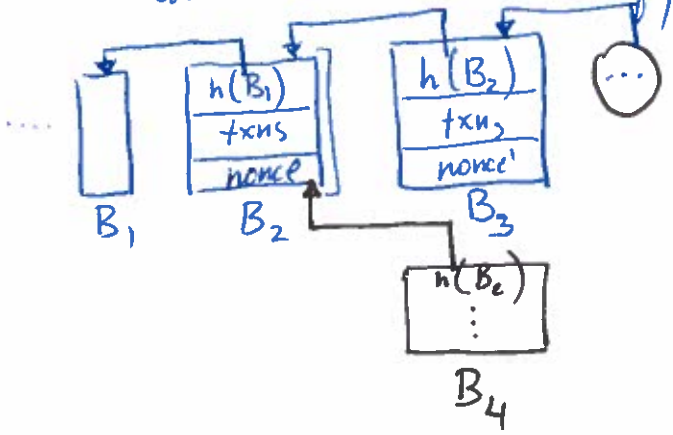
"Mining"
⇓
Reward; generates a BTC for the miner
⇓
each miner is looking for a diff. nonce
⇓
mining pools for cooperation

★ (A) Difficult to find nonce
(B) Easy to verify/check

BTC reward generated until ~2140
After that reward txn fees

Missing: ordering of txns ($txn_1 \leq_{\text{time}} txn_2$)

each block includes hash of previous block



Blockchain (actually a Tree)
- Miners only work along the longest chain
- Keep track of all forks

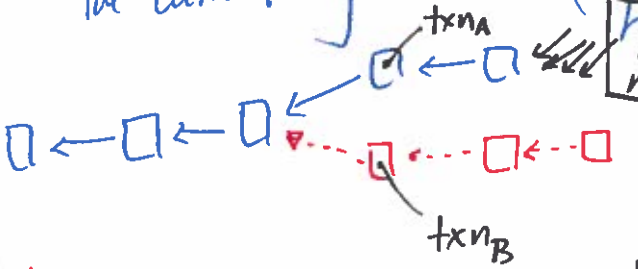
txn is not "confirmed" Unless
① It's part of the longest chain
② It must have 5 blocks that follow it
"6 confirmations"

Prob (finding nonce by A before B) ~ Relative resource Diff. btw/ A & B

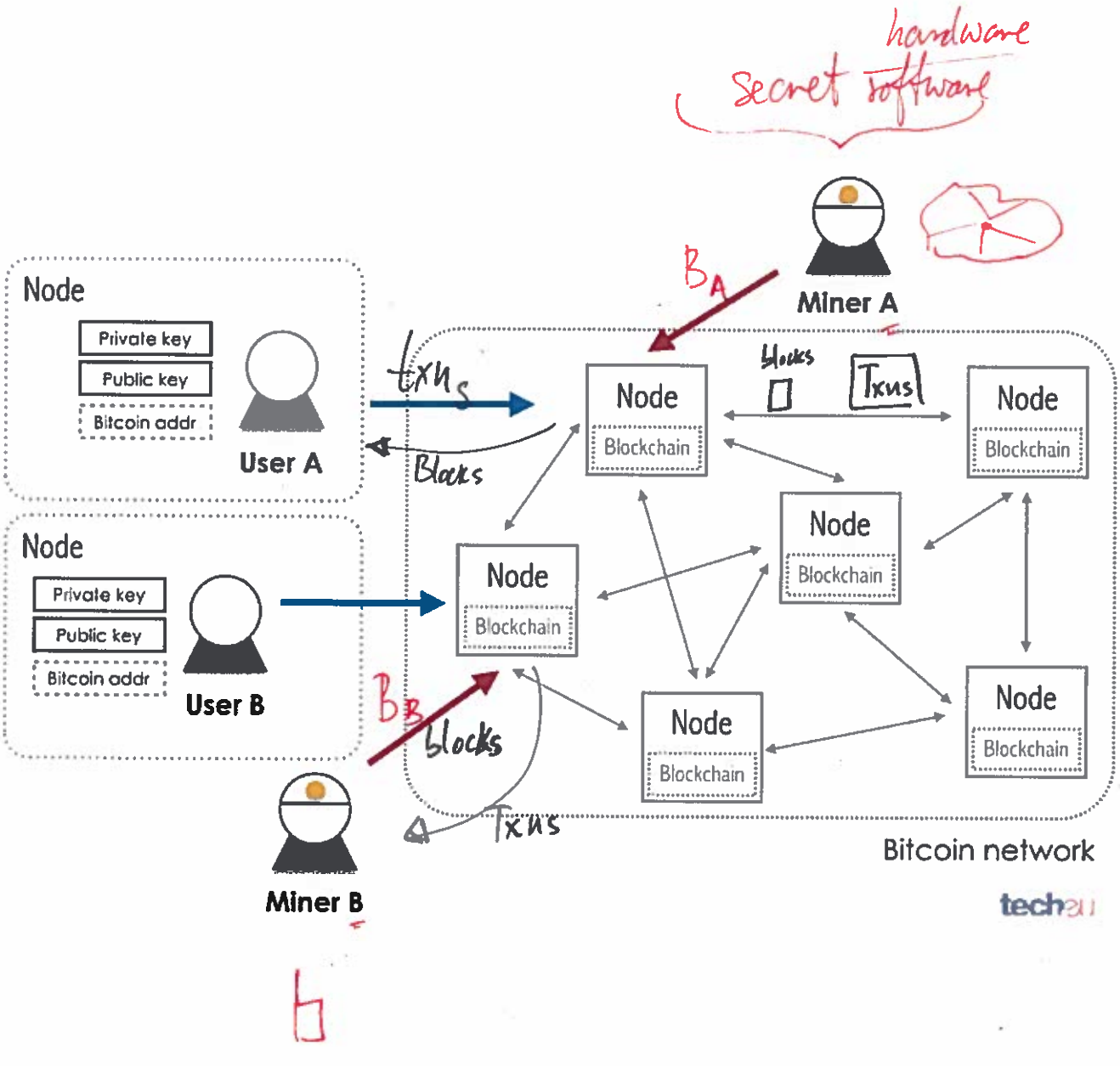
future proofing: Make difficulty change over time to reflect growing CPU power

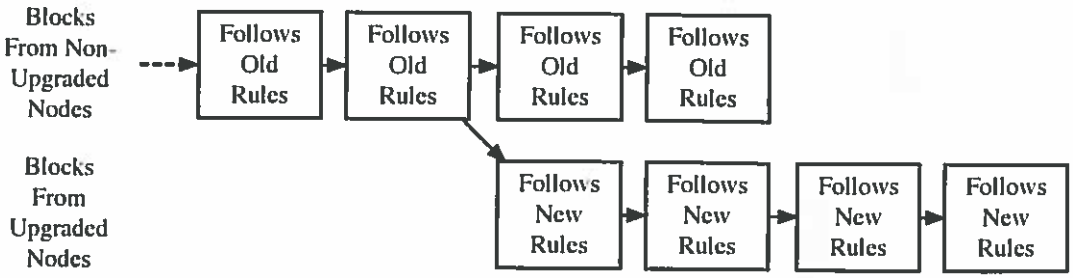
Implication of Blockchain: Only txns along longest chain matter ✲

1. Blocks are immutable: ledger → append only
2. Difficult to create a fork + get network to follow it (getting netw. to switch chains
   Requires control of enough CPU power
   ↳ to compute a competing chain that is longer than the current longest chain (Requires control of > 50% CPU power, Majority



Attacker's Goal is to add two txns : txn_A and txn_B incompatible : together spend more than 100% of an account


hardware
Secret software
Node
Private key
Public key
Bitcoin addr
User A
Node
Private key
Public key
Bitcoin addr
User B
Miner A
Miner B
txns
Blocks
Node
Blockchain
Bitcoin network
techzu



A Hard Fork: Non-Upgraded Nodes Reject The New Rules, Diverging The Chain