# Permissionless Blockchains

Attendance

MIDSEM → SAFE

Permissioned

only authorized

Consensus: RAFT, PBFT

Anyone can be Consensus Node

?? More trustworthy

PoW

# What is good about PoW?

$$Hash\Big(Hash(Prev\_Blk\_hdr) \,||\, Nonce \,||\, timestamp \,||\, BITS \,||\, MerkleRoot\Big) < target$$

Allows anyone to participate → no identity → SYBIL Attack

→ need some Compute power

Permissioned

log ← Instruction / Blk

x←3 y←5 x←x+y ..

index 1 2 3 4 → next??

A B C D E

N - participants — each 1 vote

KYC X

Permissionless (?)

20 participants

1000 clones 21st (new)

PAXOS: '80s (?) → Lamport

PBFT: '99

RAFT: → 2014

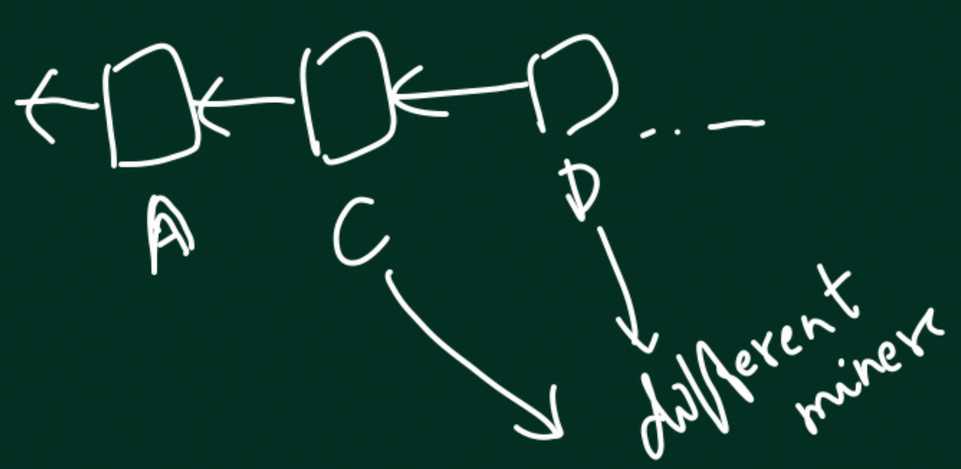
SYBIL Attack → fake identities to increase voting power

+ PoW Solved SYBIL Attack → Cannot fake compute power

1 unit of (Compute Power) ≈ 1 vote

+ No one can censor txns for very long

↳ because random winner every time

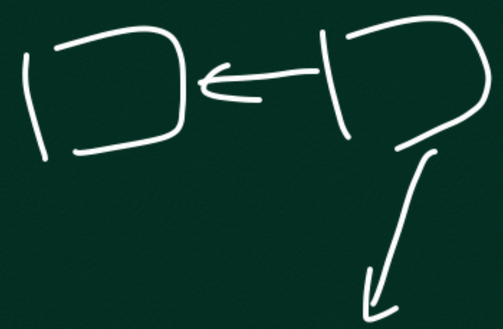


+ Fairness: fraction of blocks mined ∝ fraction of hashing power

+ Identify correct chain ← use heaviest PoW chain

# What is Bad about PoW?

→ Energy consumed



300k / 10 min → 200k / 10 min

Reward ≈ $3k / 10 min

electricity

$2k / 10 min

supply

stock / flow

51% attack easy

Litecoin

LTC

— performance (L1)

↳ Nakamoto Consensus

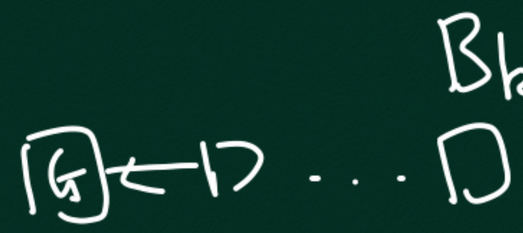
7 txs/sec

# Alternatives to PoW?

| Resource | Method to find out amt. of resoure of participant |
| --- | --- |
| Compute: CPU | PoW puzzle |
| Memory | Some algo |
| bandwidth | " |
| Secure hardware | " |

# Virtual Resource

↳ resoure on blockchain




## Proof of stake

PoS

+ no energy consumed

| stake ( #tokens ) | Pub. Key | frac. of blks mined |
|---|---|---|
| $x_1$ | $PK_1$ | $\frac{x_1}{X}$ |
| $x_2$ | $PK_2$ | $\frac{x_2}{X}$ |
| ⋮ | ⋮ | ⋮ |

$PK_2 \rightarrow PK_2^{(1)}, PK_2^{(2)}, \ldots$

$X = \sum_i x_i$

- random winner (?)
  - SYBIL Attack (?) → Solved
    - Can anyone participate — YES → Buy Tokens
      - Identify correct chain easily (?)
    - Fairness (?) — if prop. ∧ blks mined to stake
    - Incentives — mining reward

Naive PoS , Ethereum PoS (2.0) , Algorand

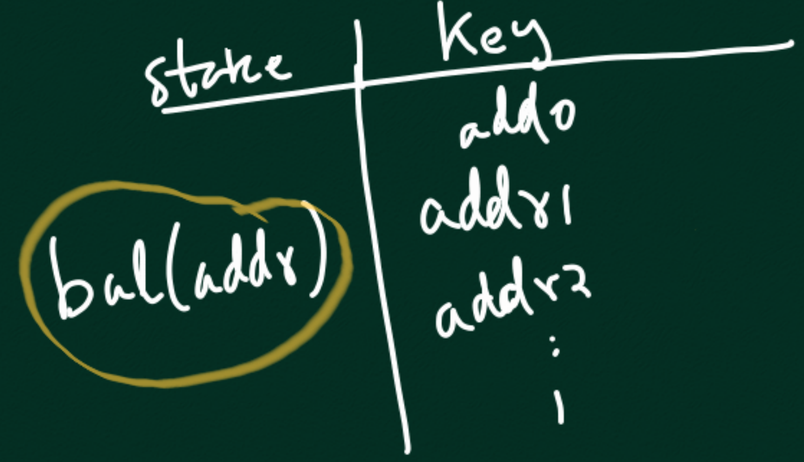
PoW: $\text{Hash}\Big(\text{Hash}(\text{Prev}) \,\|\, \text{Nonce} \,\|\, \text{Bits} \,\|\, \text{Timestamp} \,\|\, \text{Merk.Root}\Big) < \text{target}$

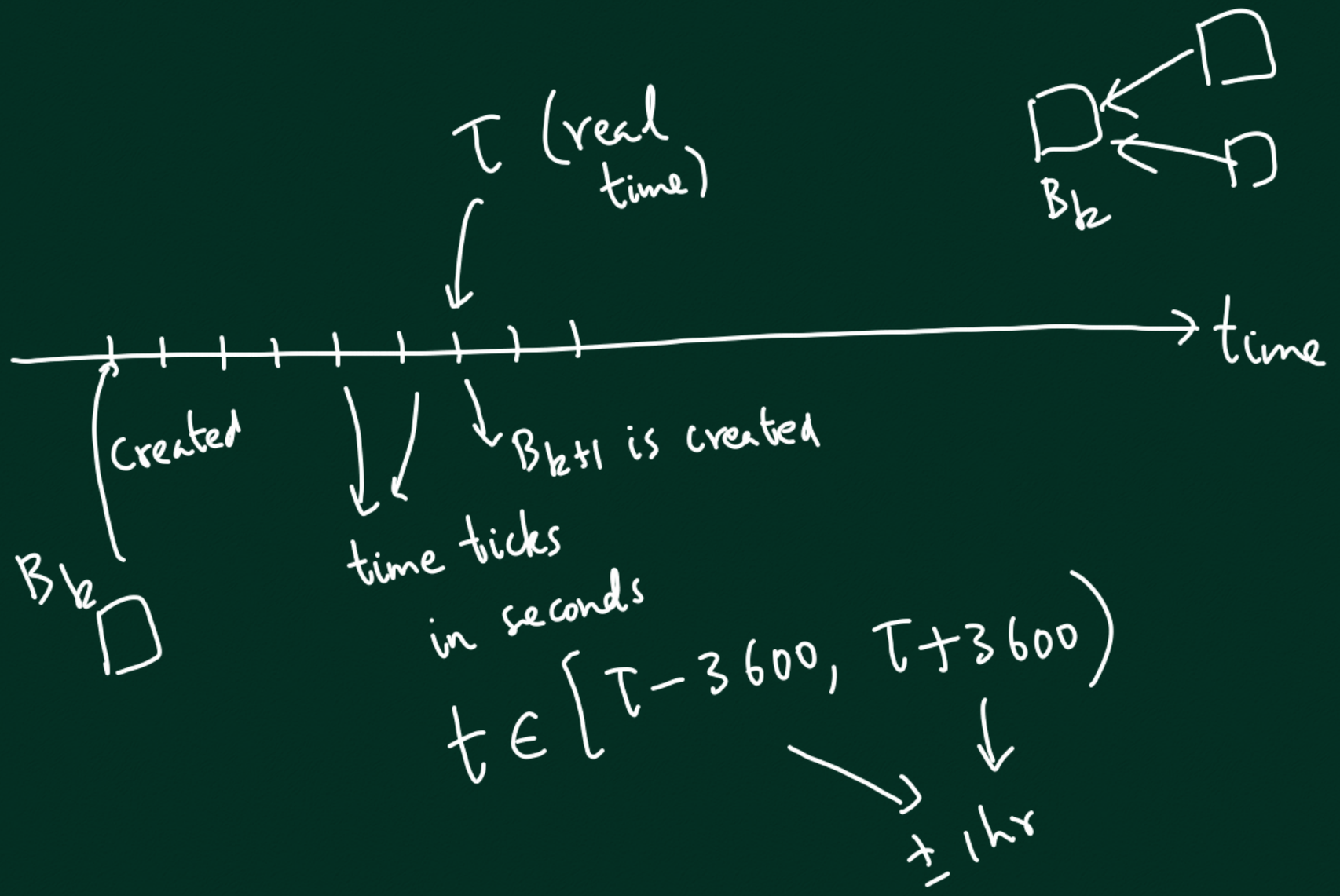
Hdr

Micali (Turing award)

Naive PoS

$$\text{Hash}\Big(\text{Hash}(B_k\text{-Hdr}) \,\|\, \text{addr} \,\|\, t_{\text{timestamp}}\Big) < \text{target} \times \text{bal}(\text{addr})$$


T (real time)
time
Created
$B_k$
$B_{k+1}$ is created
time ticks in seconds
$t \in [T-3600, T+3600)$
$\pm$ 1hr
$B_k$