Proof of Stake

Attendance

CPU — PoW

RAM

Bandwidth(?)

⋮

Virtual Resources

Stake

Tokens

$PK_1 \rightarrow x_1$

$PK_2 \rightarrow x_2$

⋮

$\frac{x_1}{X}$ $\frac{x_2}{X}$ ⋮

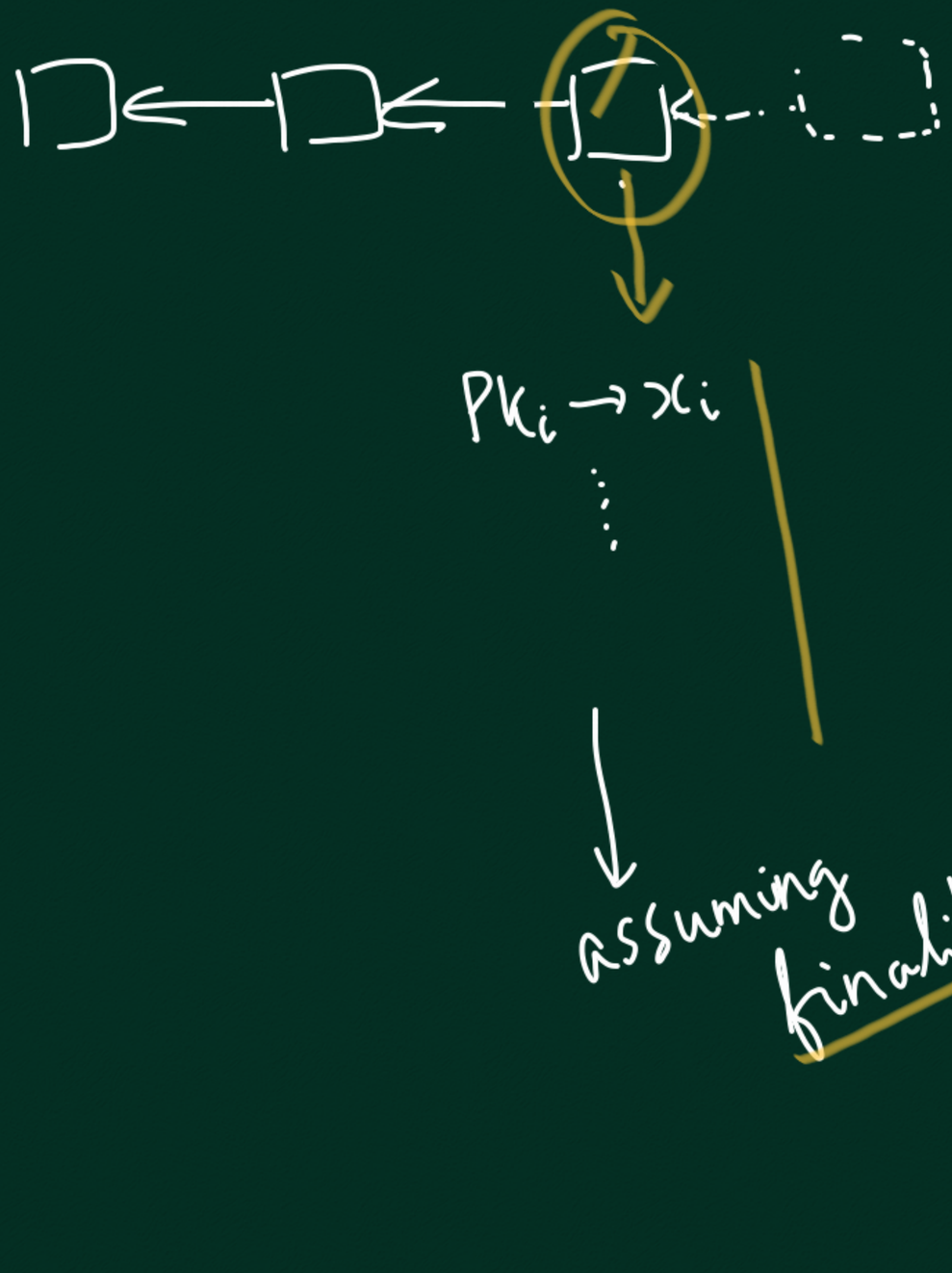
$\sum_i x_i = X$

Extra (Class SHIFTED Oct 15 Wed??)

Issues with using STAKE

- How to start mining?
  ↳ someone with no stake needs to buy some

- How to identify correct public chain?
  ↳ no concept of heaviest chain

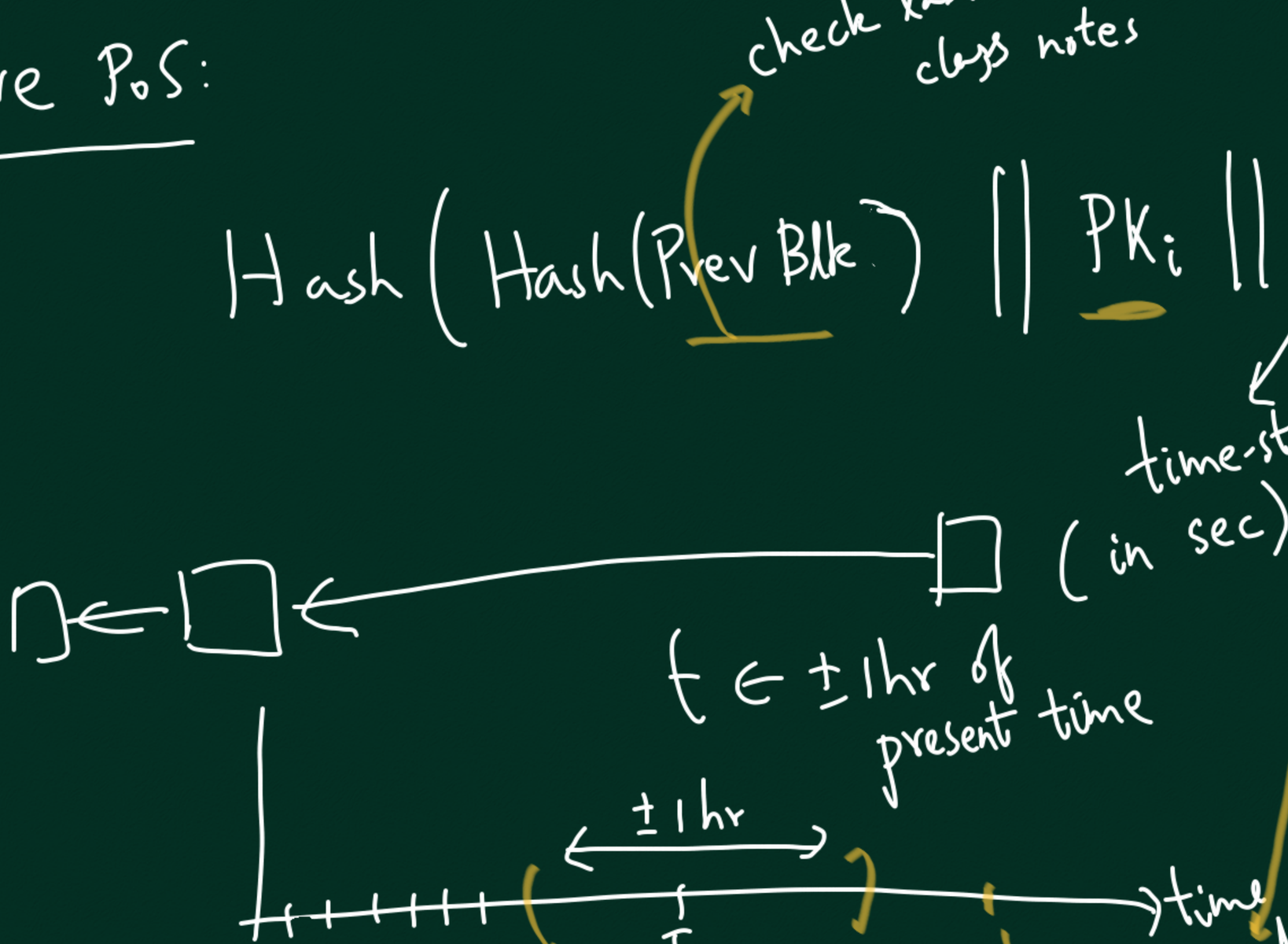

$pk_i \to x_i$
assuming finality

Naive PoS:

check last clock notes

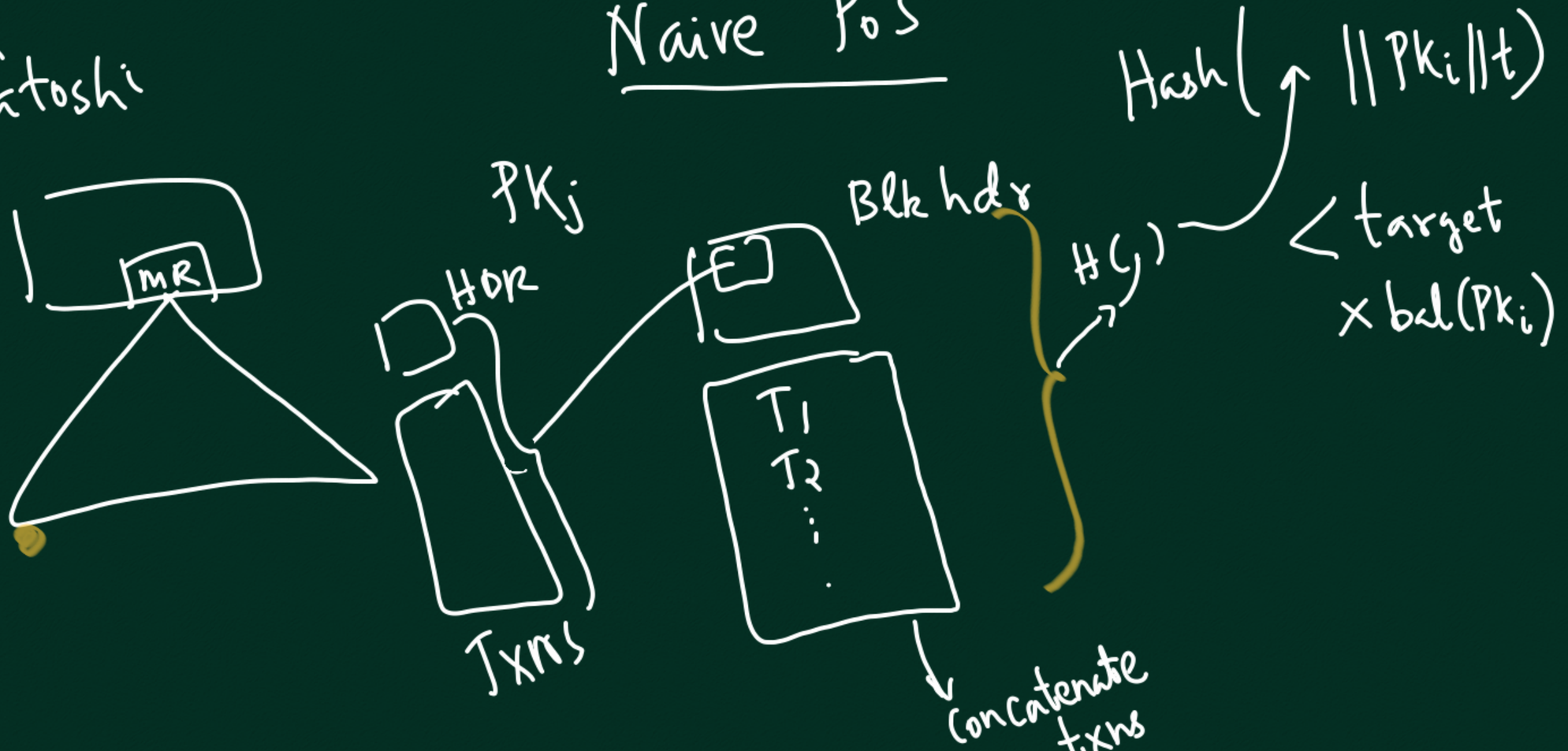
$$\text{Hash}\Big(\text{Hash}(\text{Prev Blk}) \;||\; PK_i \;||\; t\Big) \leq \text{target} \times \text{bal}(PK_i)$$

time-stamp (in sec)



How to connect txns to blk??

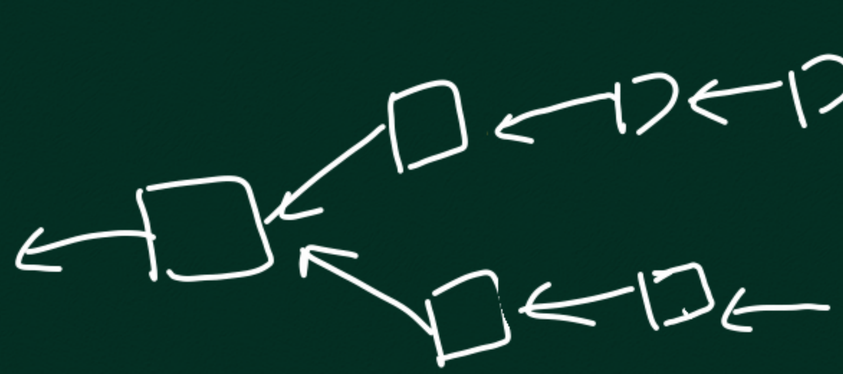
Naive PoS



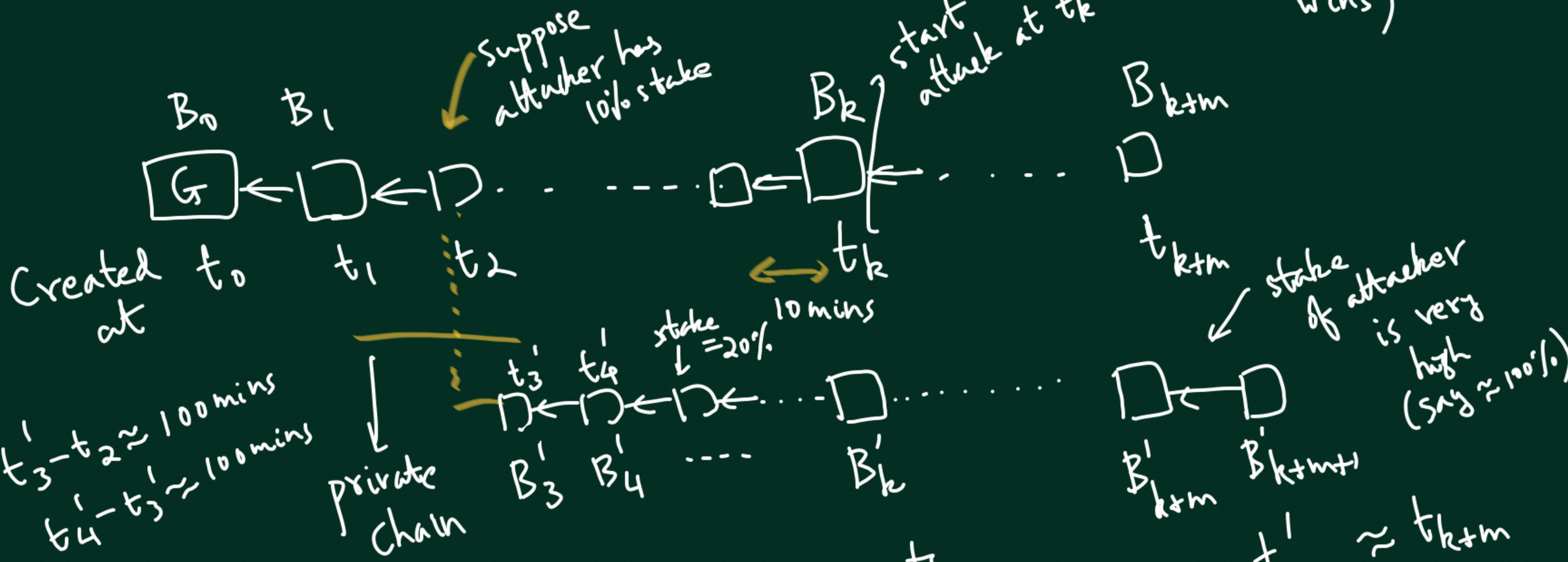
Problems with Naive PoS

1. Nothing at stake

Nothing to lose by extending both branches



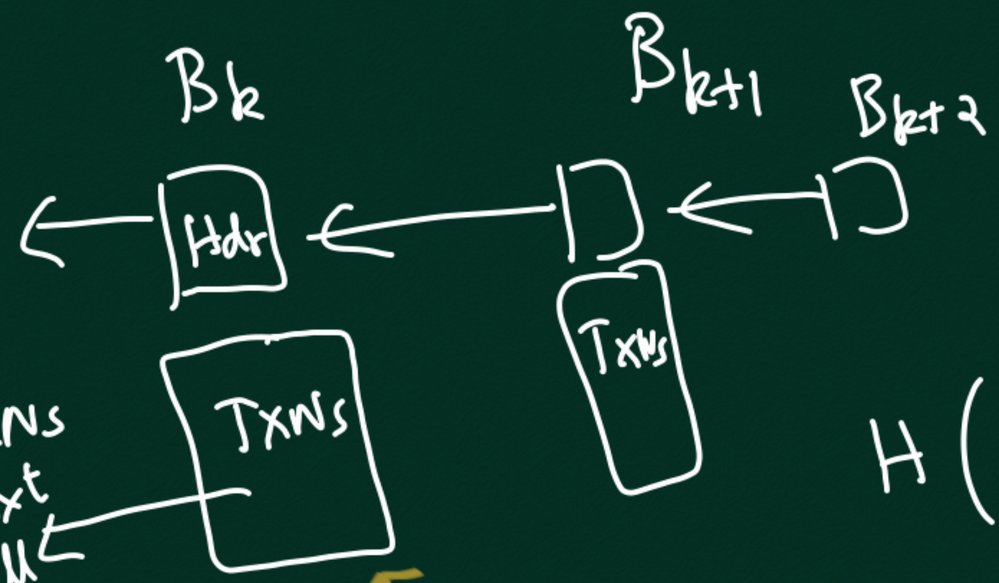
2) Long-range attack (Suppose longest chain wins)



Mining fees: Like Bitcoin, miner gets some mining reward + txn fees

+ txn

3) Pre-computing attack



(i) modify Txns to become next leader as well

(ii) then release B_k

$H\left(H(B_{k-1}) \,||\, PK_j \,||\, t\right) < \text{target} \times bal(PK_j)$

Solved by owner of PK_j

$H\left(H(B_k) \,||\, PK_j \,||\, t\right) < \text{target} \times bal(PK_j)$

entire B_k

(4) Initial Distrib. problem

Initial Stake → ??

After some time

$x_1 \longrightarrow x_1+y_1 \approx \frac{x_1}{X} \approx \frac{x_1+y_1}{X+y}$

x_2

$\vdots$

$\frac{x_{10}}{\text{Initial } X \text{ total}} \longrightarrow \frac{x_{10}+y_{10}}{X+y}$

y_{10}: txn fees + mining reward

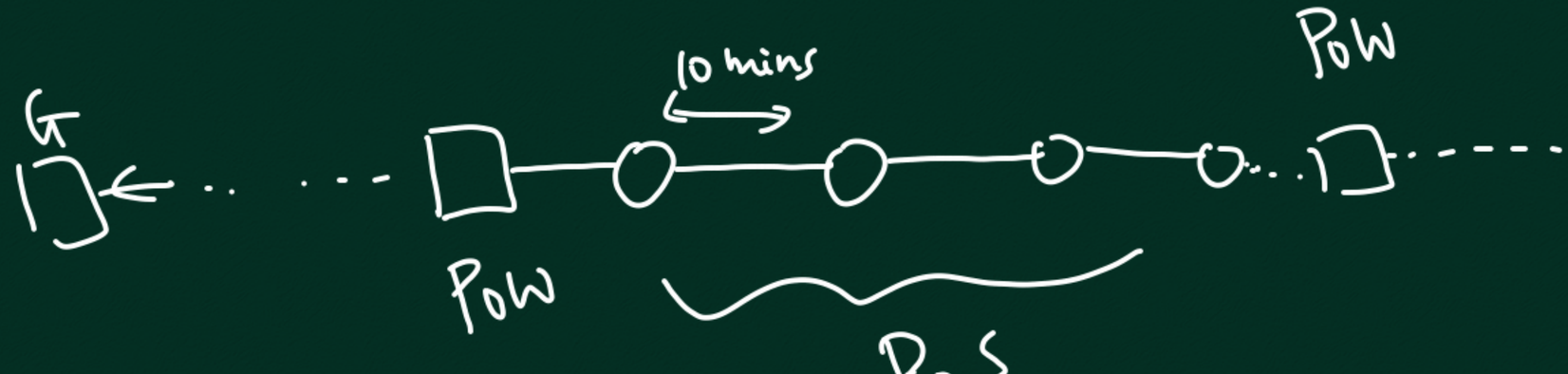
S.o. miners may not want to spend money so that he can keep getting mining rewards

Solutions

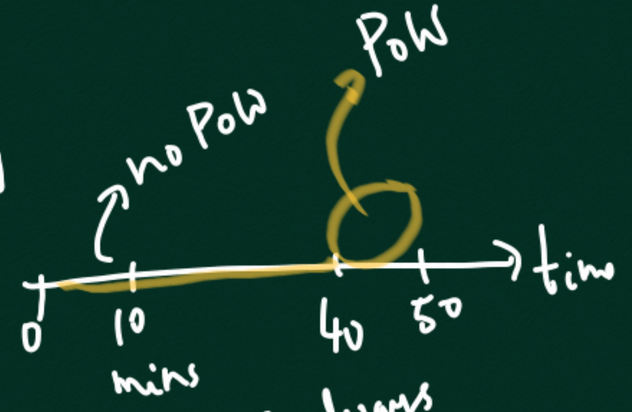
2014 SLASHER

Combinations of PoW + PoS

(1)

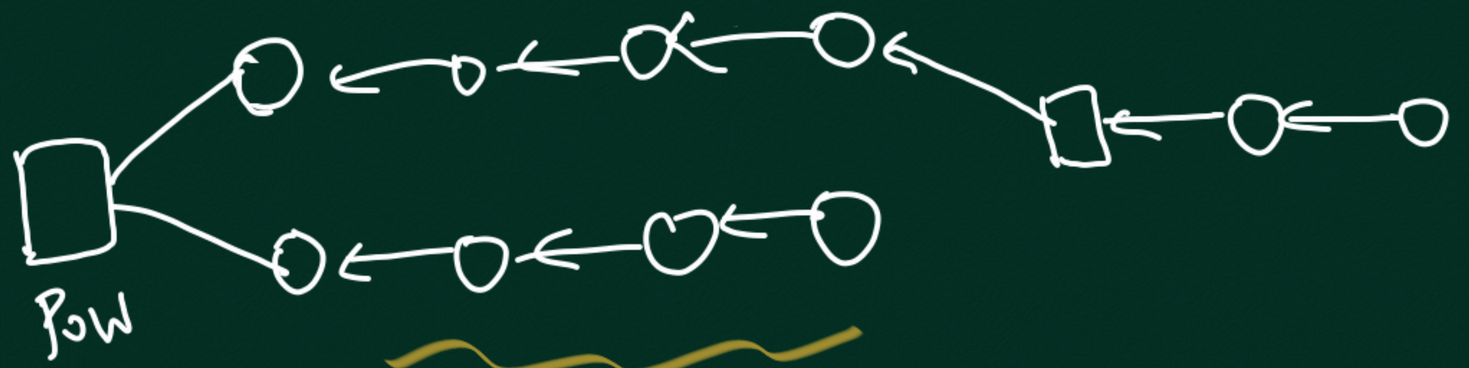


Every n^{th} blk is created by PoW



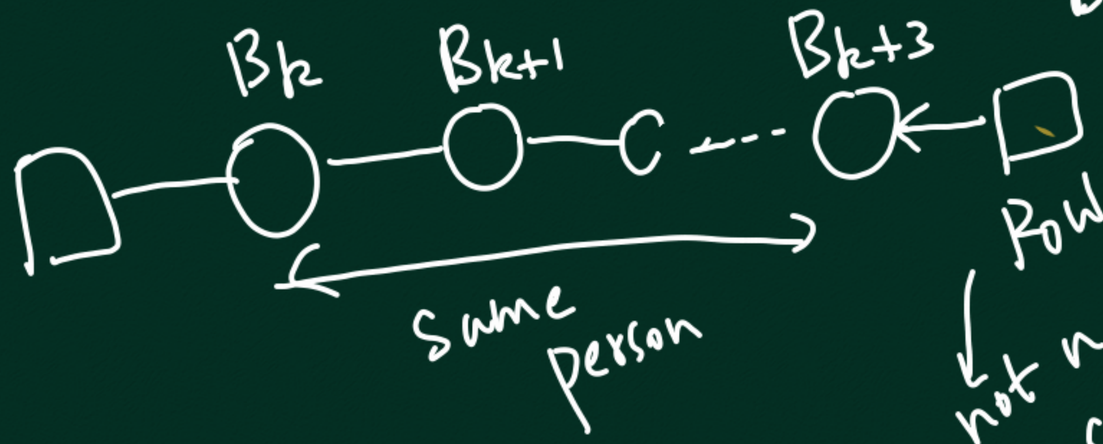
Naive PoS (?)

Long-Range (?)



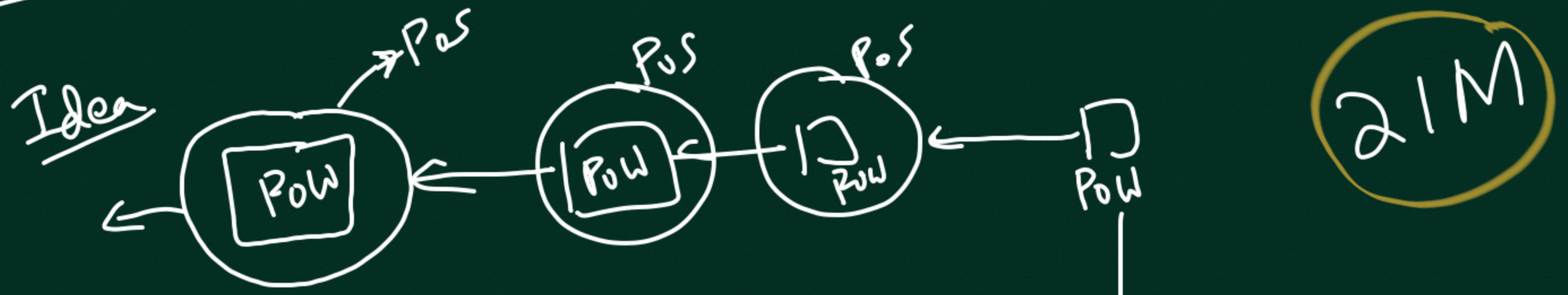
Nothing at stake → persists only for n-consec blks

Pre-computing?



Hybrid PoW+PoS still uses energy, but could be less than a pure PoW chain (assuming same hashing power in both chains)

Vitalik Buterin (SLASHER)

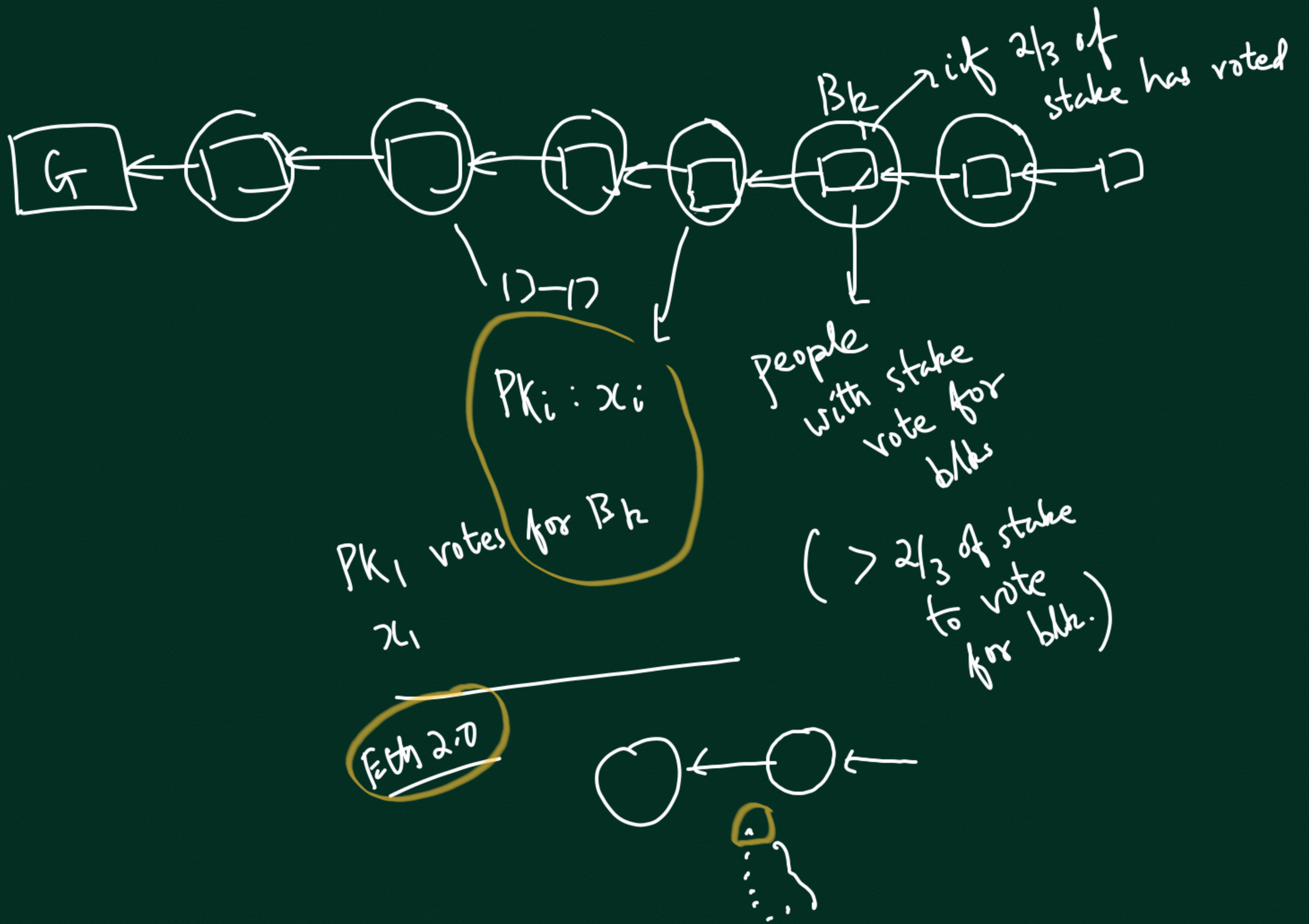


- target
- mining reward

Bitcoin: ½ every 4 years

SLASHER: 1/50 every YEAR

uses very less energy


G
Bk
if 2/3 of stake has voted
12-17
$Pk_i : x_i$
Pk_1 votes for B_k
x_1
People with stake vote for blks
(> 2/3 of stake to vote for blk.)
Eth 2.0