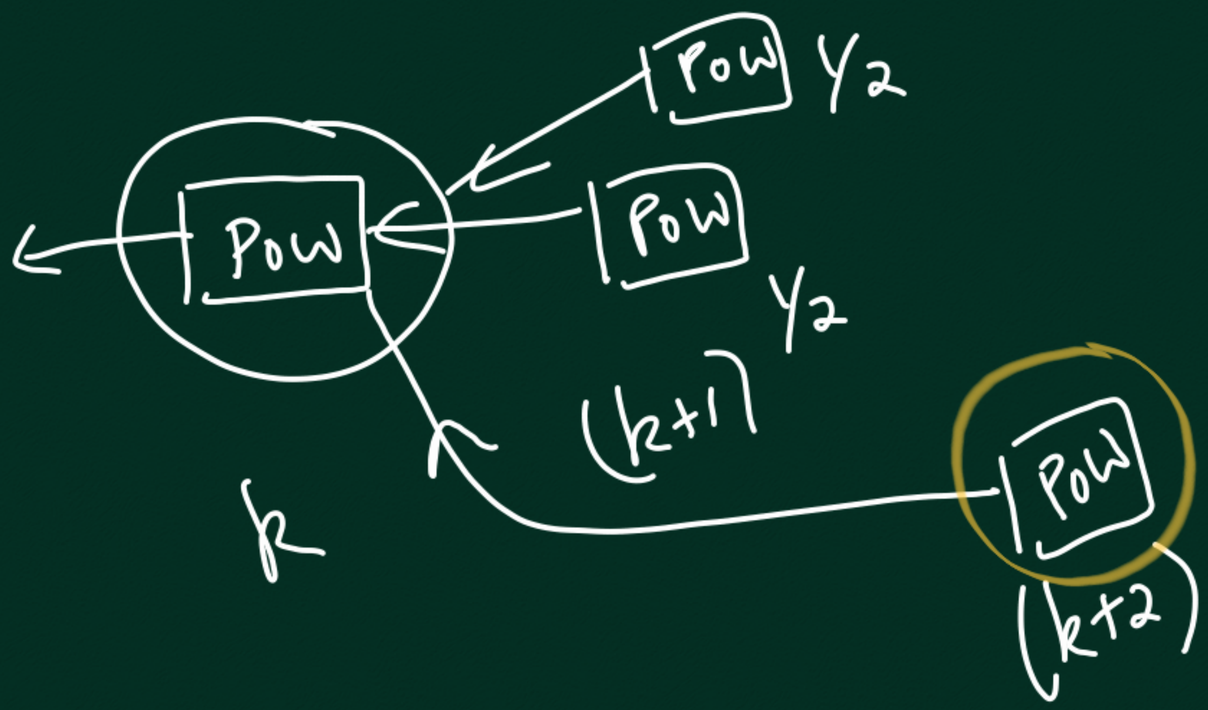
PoS

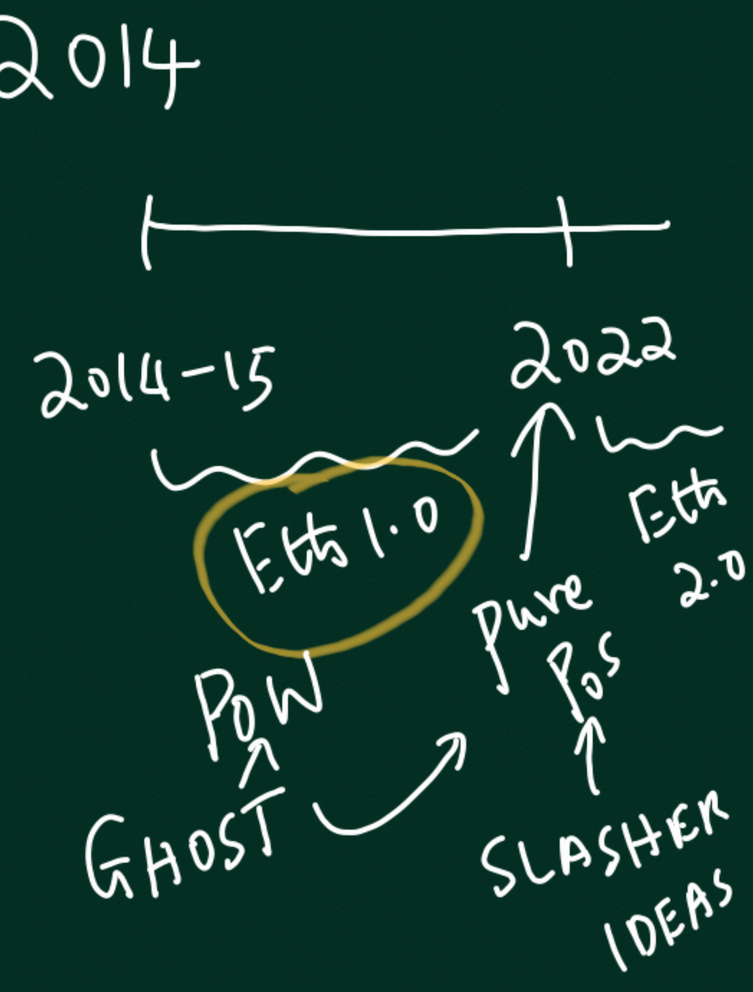
Attendance

Naive PoS

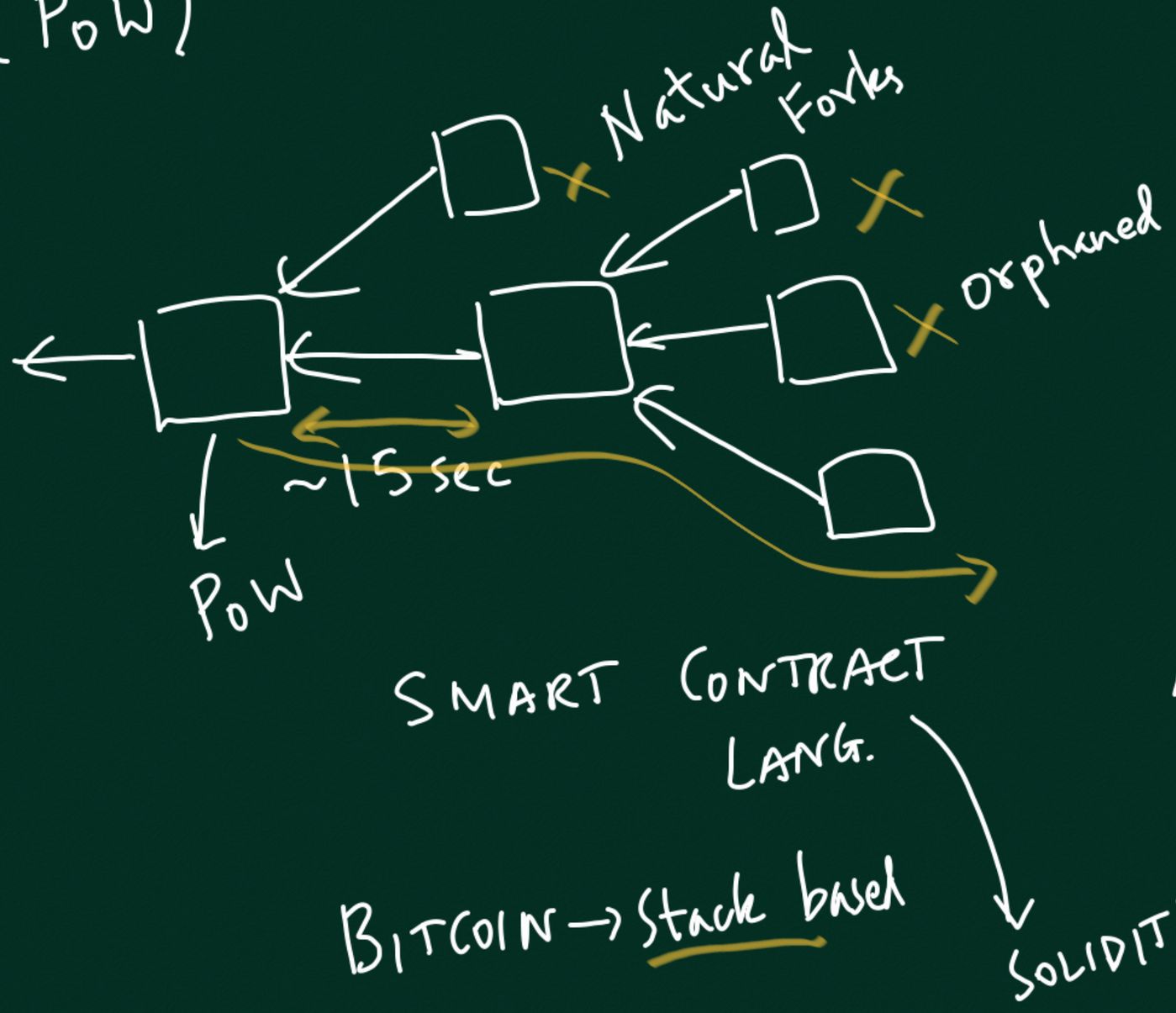
PoW + PoS → N^{th} blk PoW

→ SLASHER





Eth 1.0 (PoW)

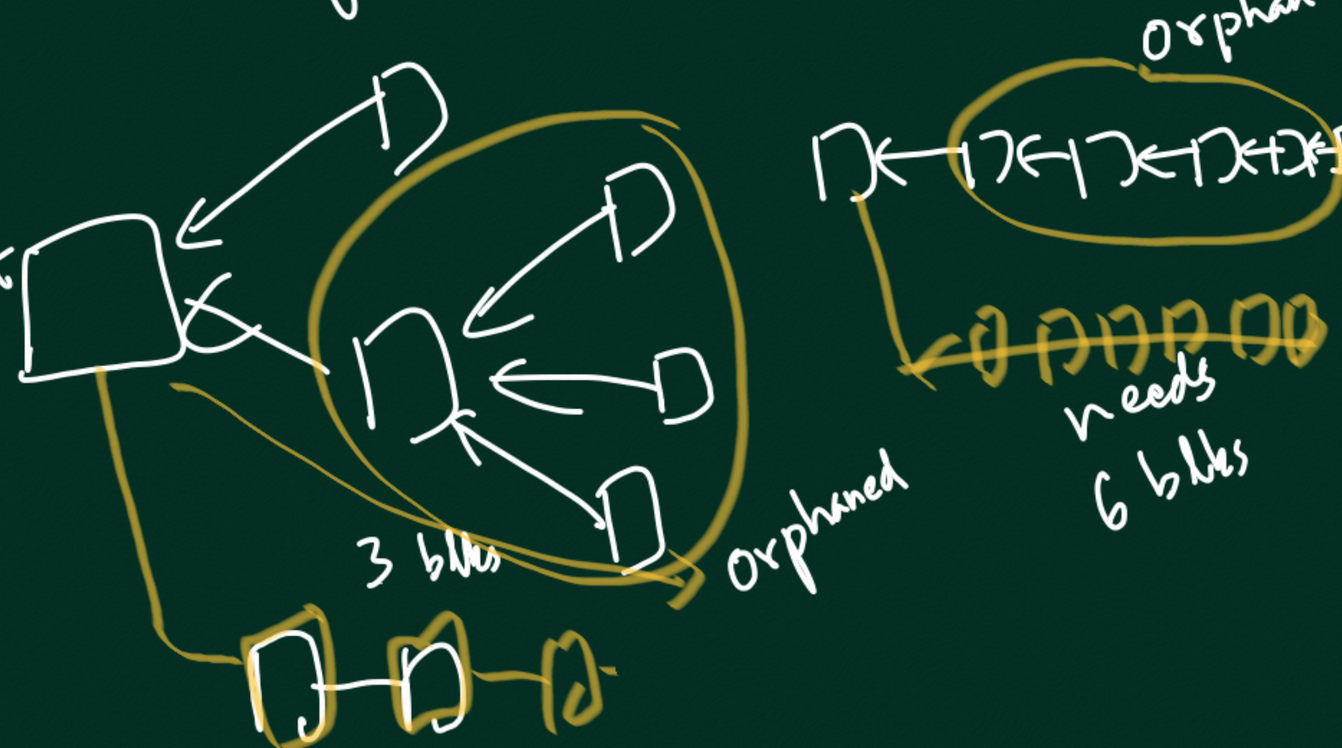

Natural Forks
orphaned
~15 sec
PoW
SMART CONTRACT LANG.
ASIC resistent
BITCOIN → Stack based
SOLIDITY

Issues

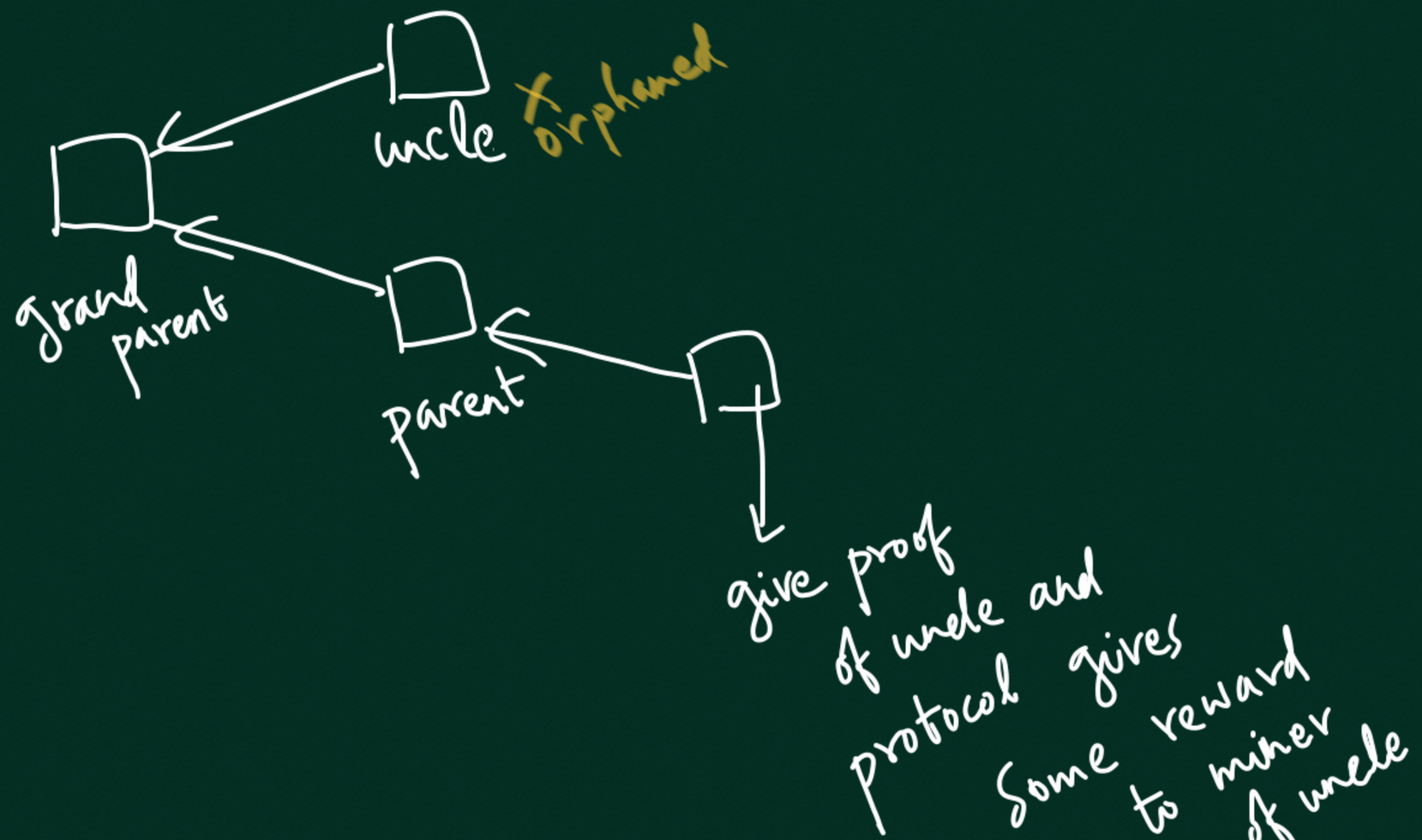
1. Too many blks orphaned → how to incentivize miners who may mine orphaned blks

2. Attacks become easier if more forking occurs
   ↓
   Private chain

Satoshi's longest/heaviest chain rule

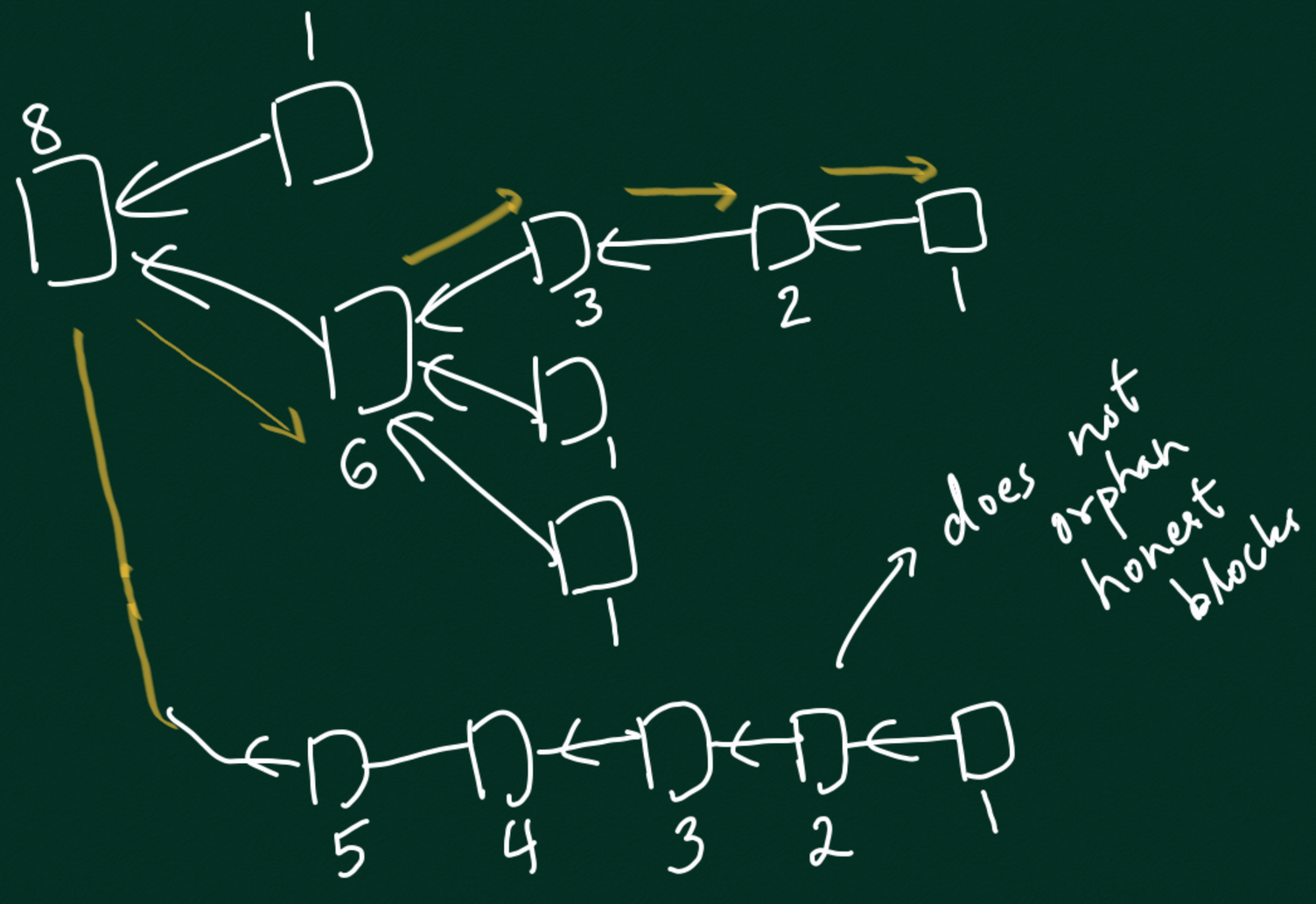


Soln 1: Uncle Rewards



Soln 2: GHOST

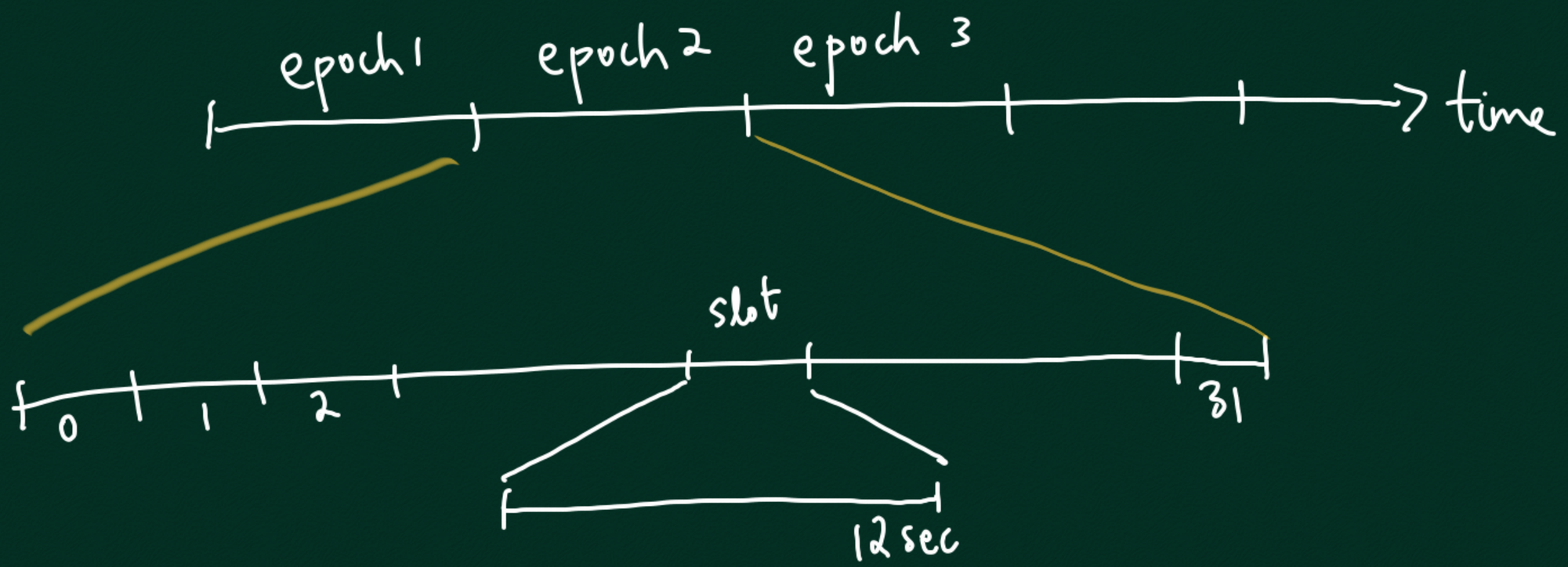
Greedy Heaviest Observed Sub-tree



Eth 2.0 : Pure PoS

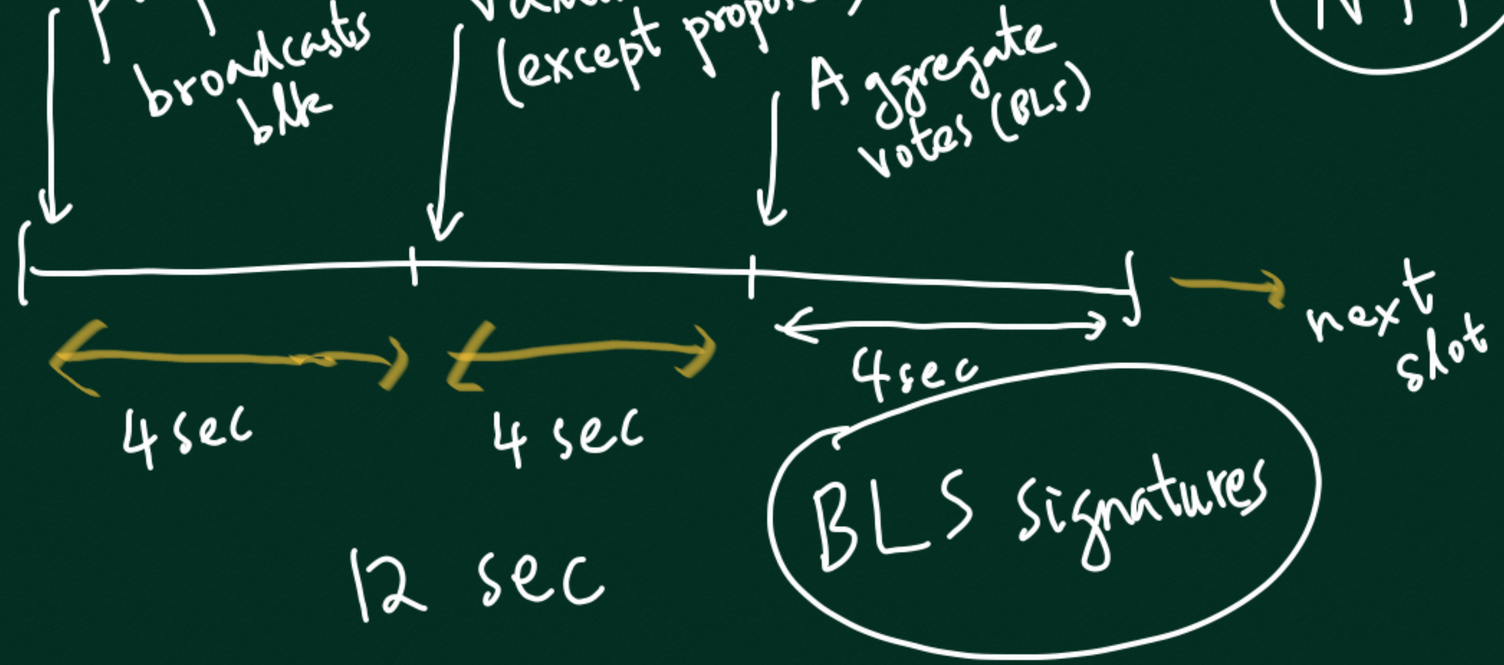
GHOST

SLASHER
(Committees, Slashing)



- Form Committee for each slot, based on stake
  - 1 committee member (validators) proposes blk
    - rest of members vote for a blk in that slot

Size ≈ 1000's



12 sec

NTP

How to select Committee?

- Deposit 32 ETH to become validator
  - → handle SYBIL
  - → can be SLASHED
    - → gen. multiple blks in single slot
    - → vote for multiple blks in same slot

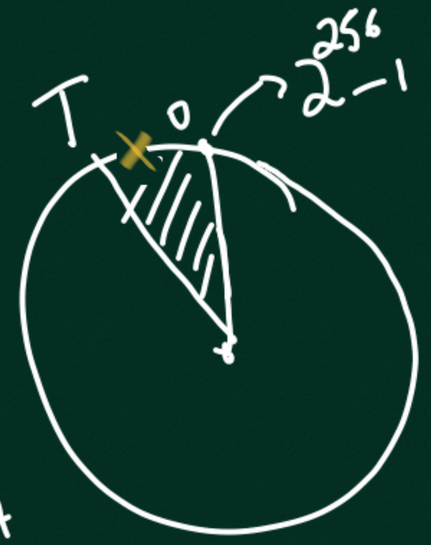
each validator assigned to 1 epoch

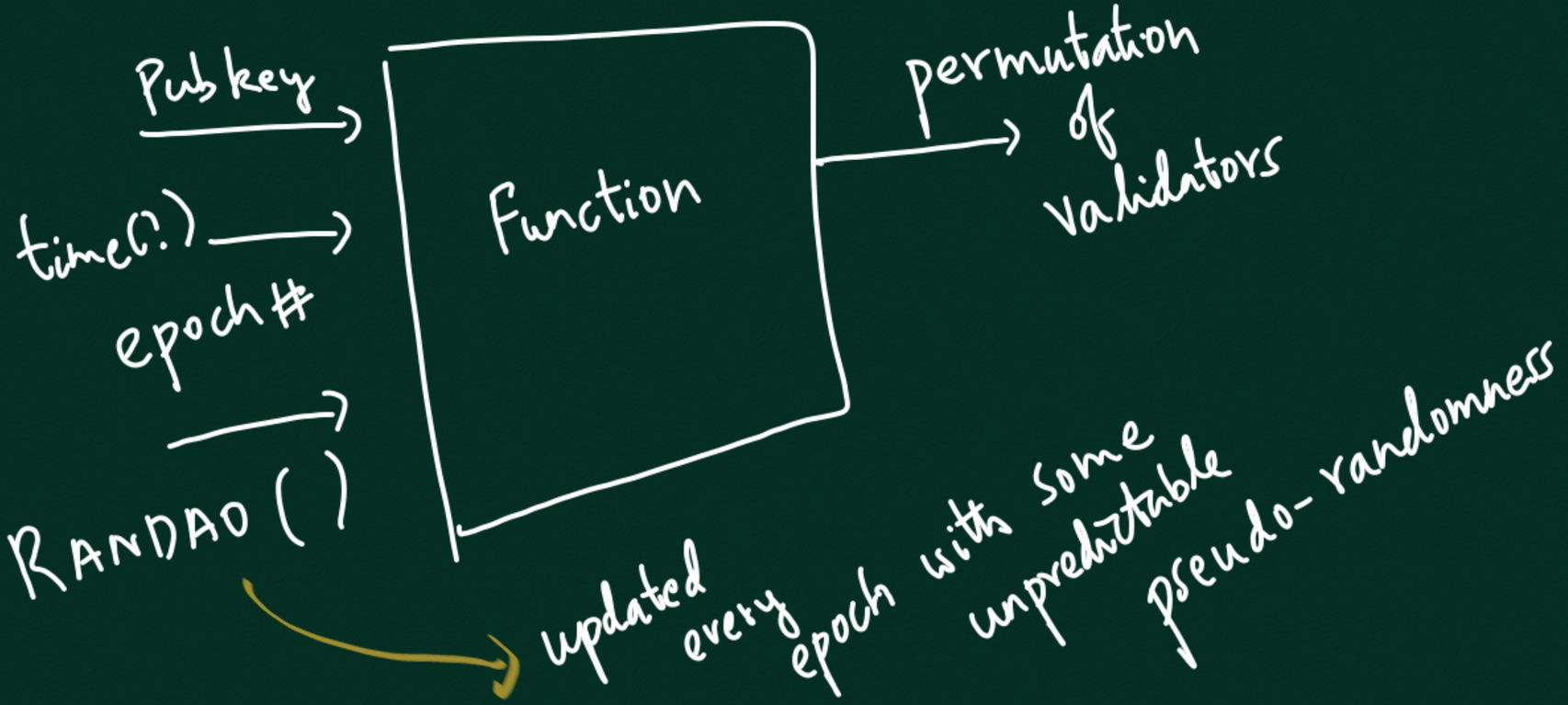
Committee in an epoch

Randomness (?)

Validator: Pubkey , Privkey , Stake

≃ 32 ETH





RANDAO()

$R_1 = R_0 \oplus r_0$

RANDAO update → $R_{32} = R_{31} \oplus r_{31}$

0 1 2 ... 31

$R_0 = \text{RANDAO}()$

r_0 r_1 r_2

R_{30} R_{31}

k slots

2^k

$R_{n+1} = R_n \oplus r_n$

must be in blk.

$H(\text{Sign}(\underbrace{\text{epoch\#}}_{\text{msg}}, \text{priv\_key}))$

of proposer of blk

all honest, net. delay < 4s

net. delay is large

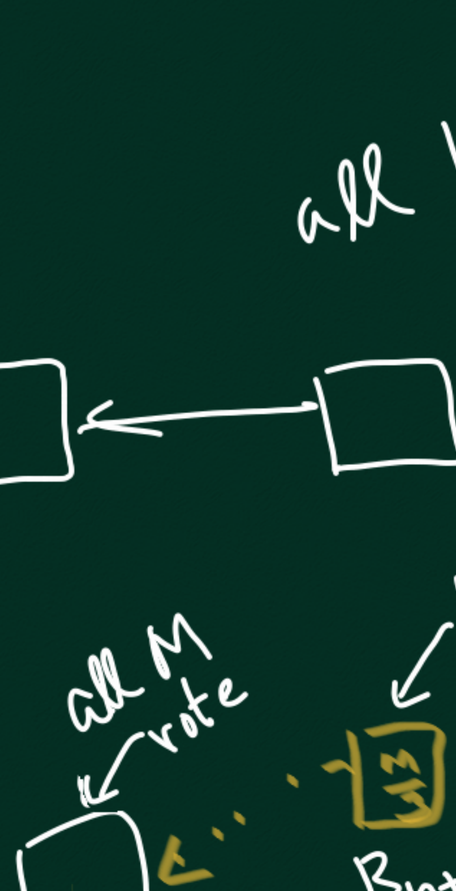
all M vote

own (B_n)

$\left(\frac{M}{3}+\frac{2M}{3}\right)$

$+\frac{M}{3}$

B_{n+1}

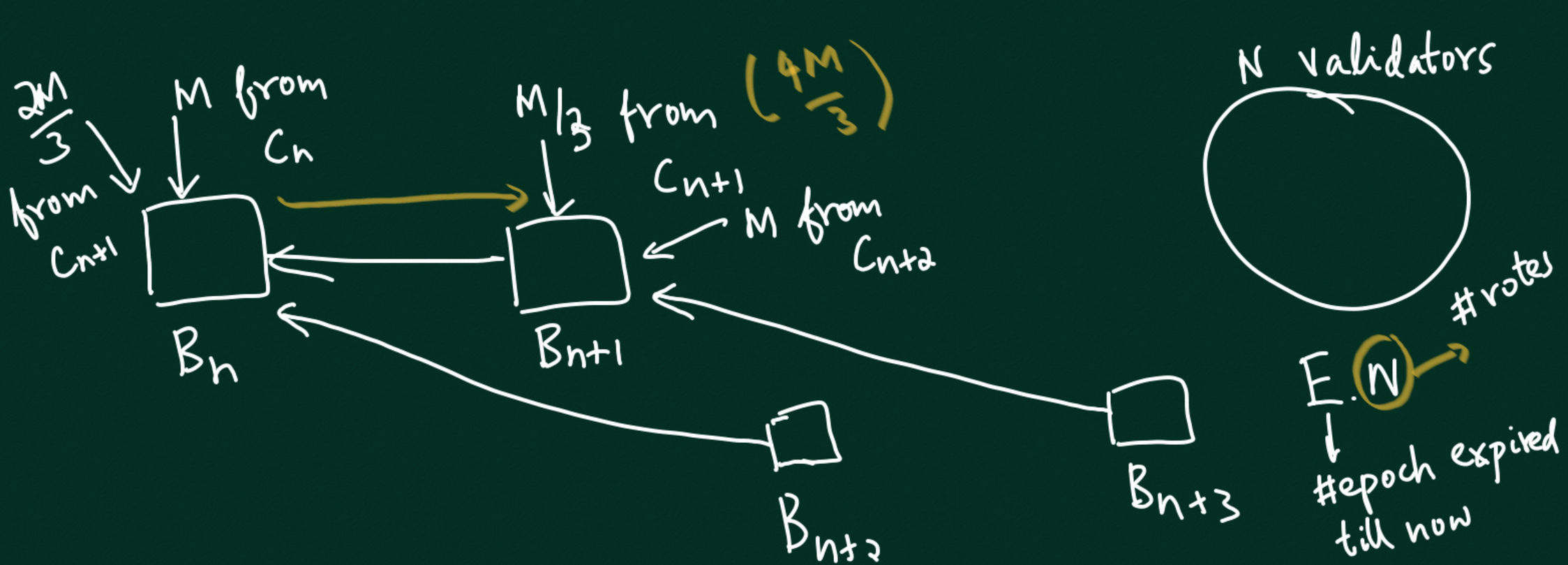


How to deal with forks?

(let's use GHOST)

DoS

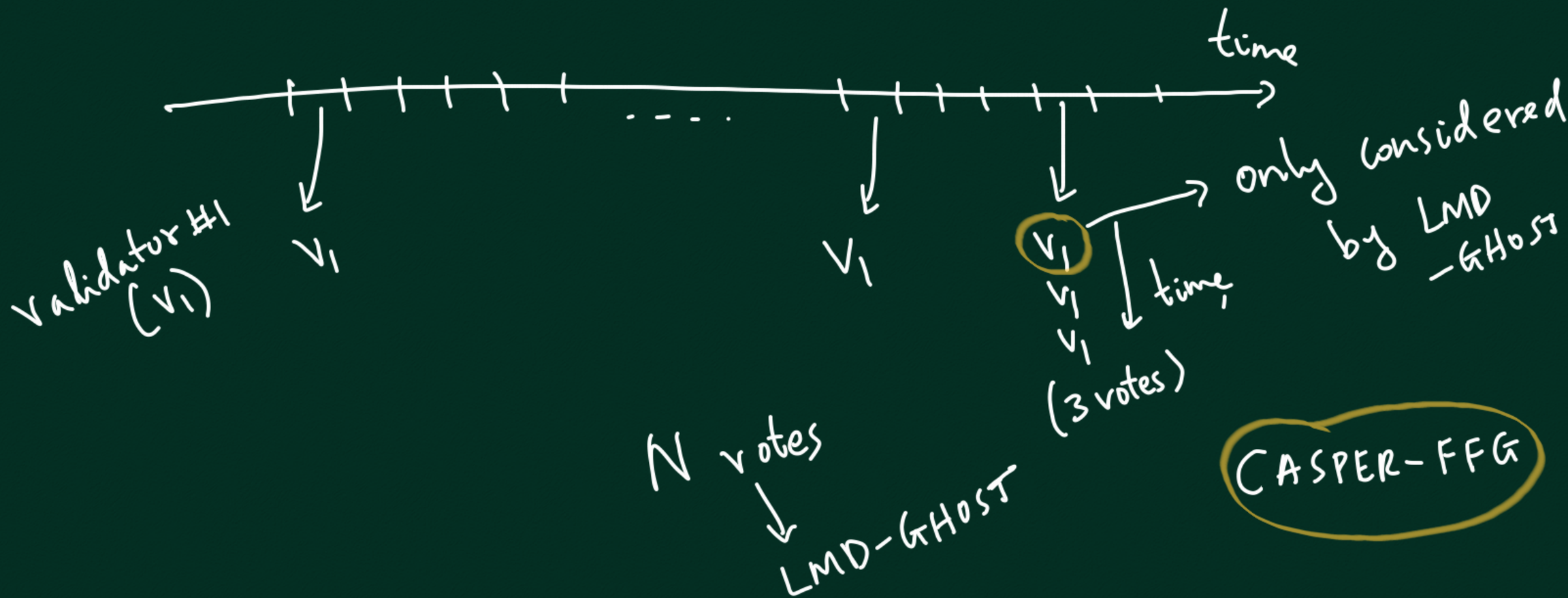
Use GHOST to vote for B_{n+1}



LMD - GHOST

→ Latest Message Driven

(Don't consider all votes of a particular validator;
only consider 1st seen vote from
a validator in most recent slot
he has voted in)


time
Validator #1
(v_1)
v_1
v_1
v_1
only considered by LMD-GHOST
time
v_1
(3 votes)
N votes
LMD-GHOST
CASPER-FFG