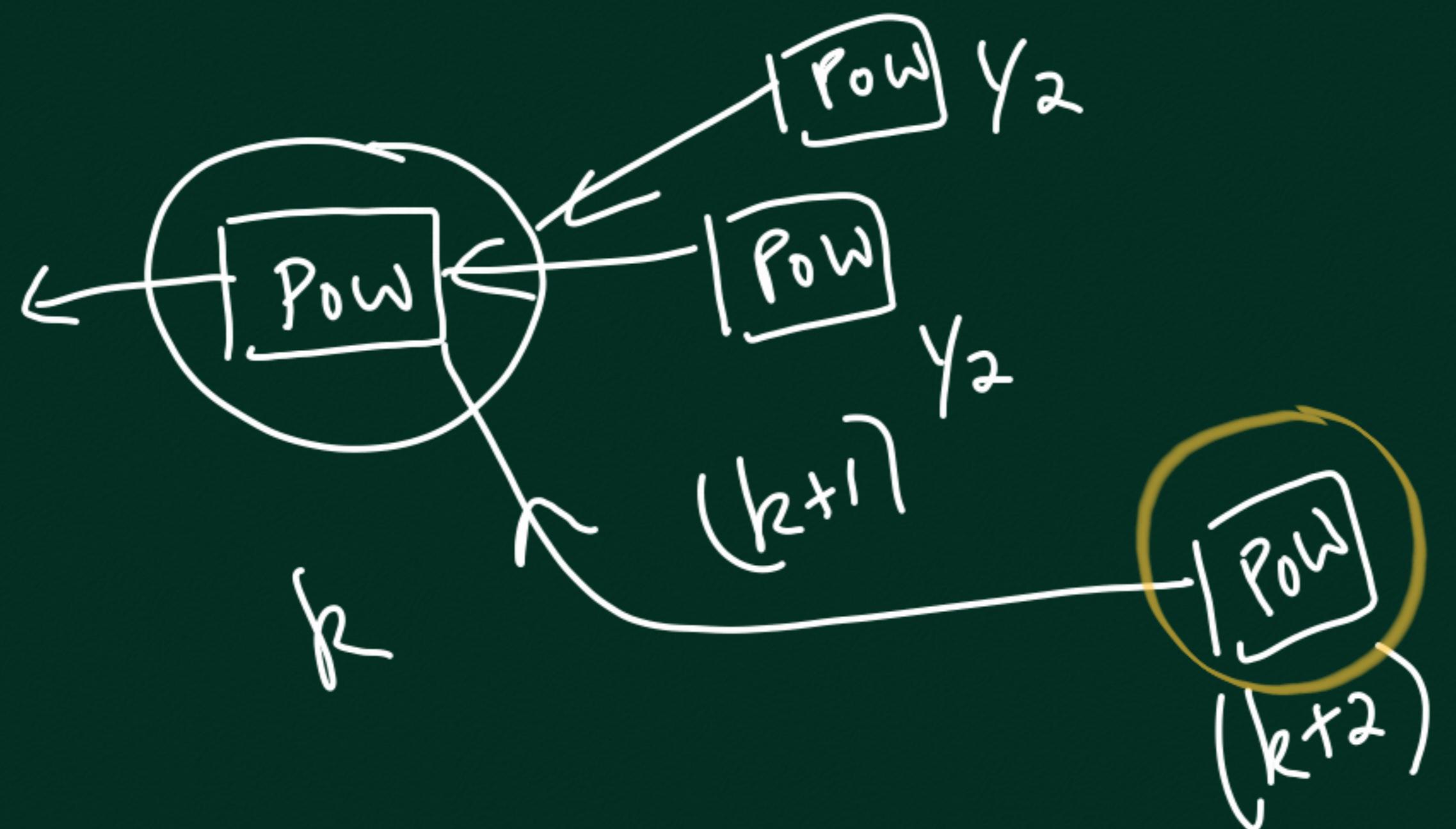
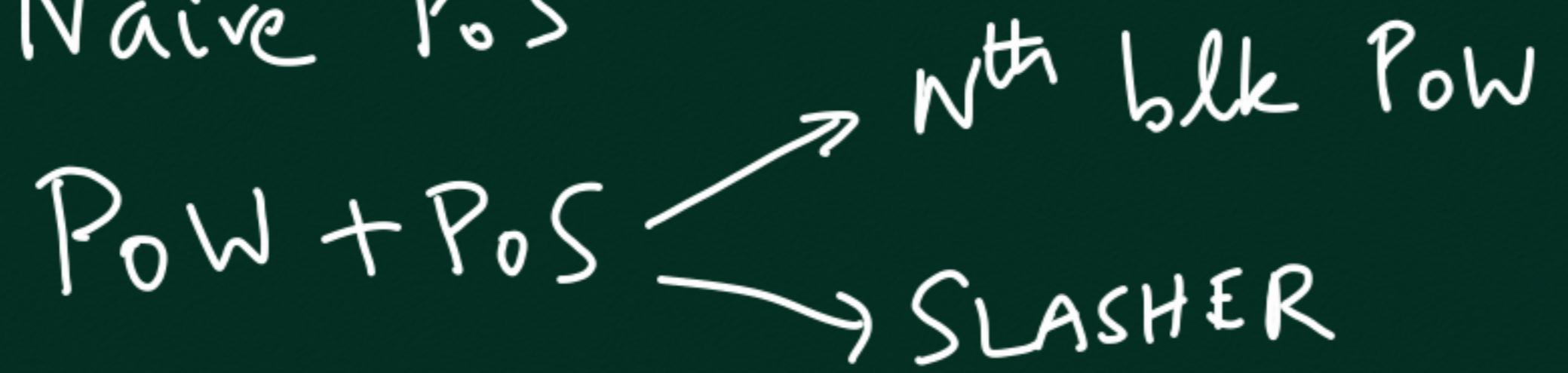
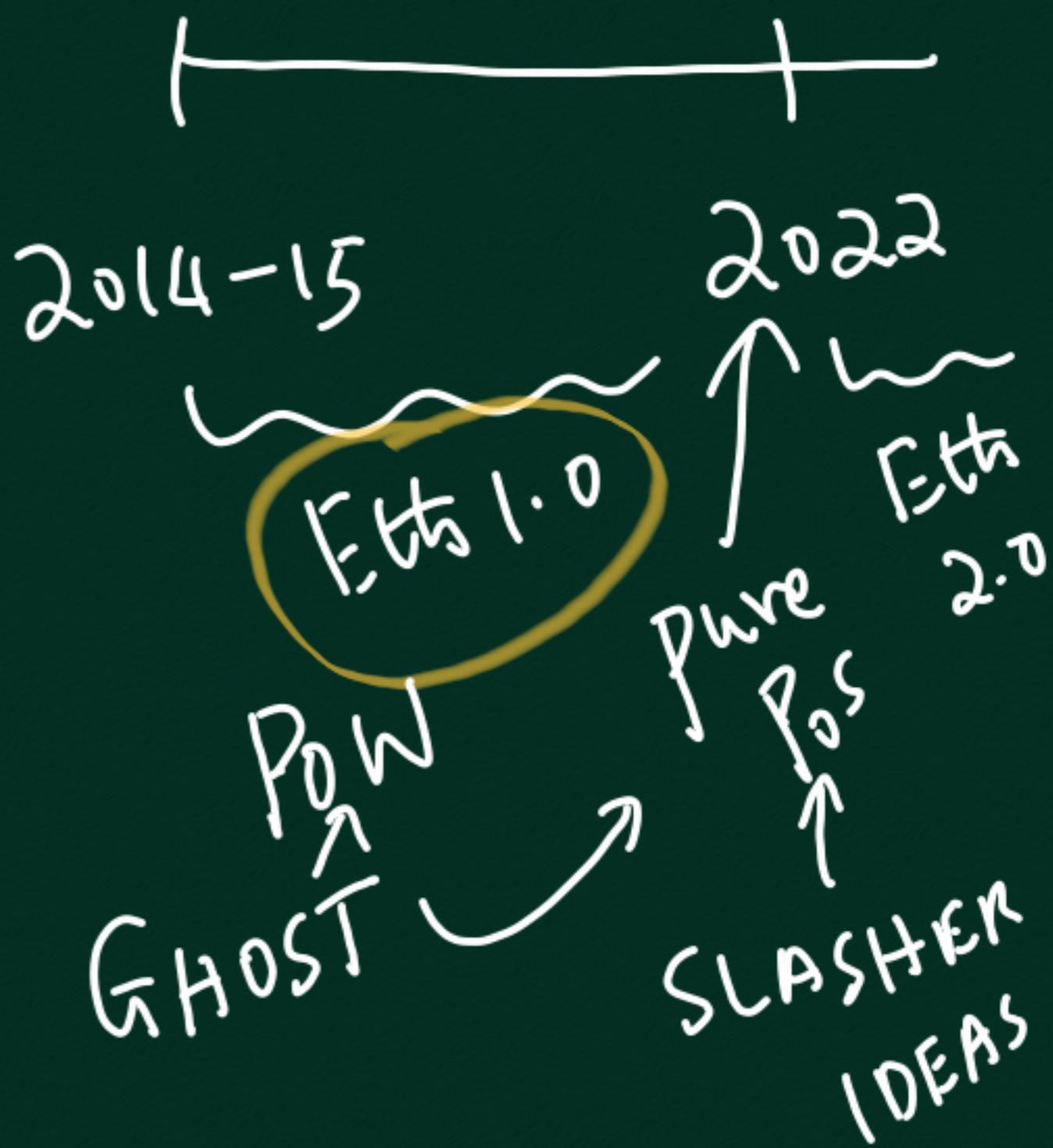


PoS

Naive PoS

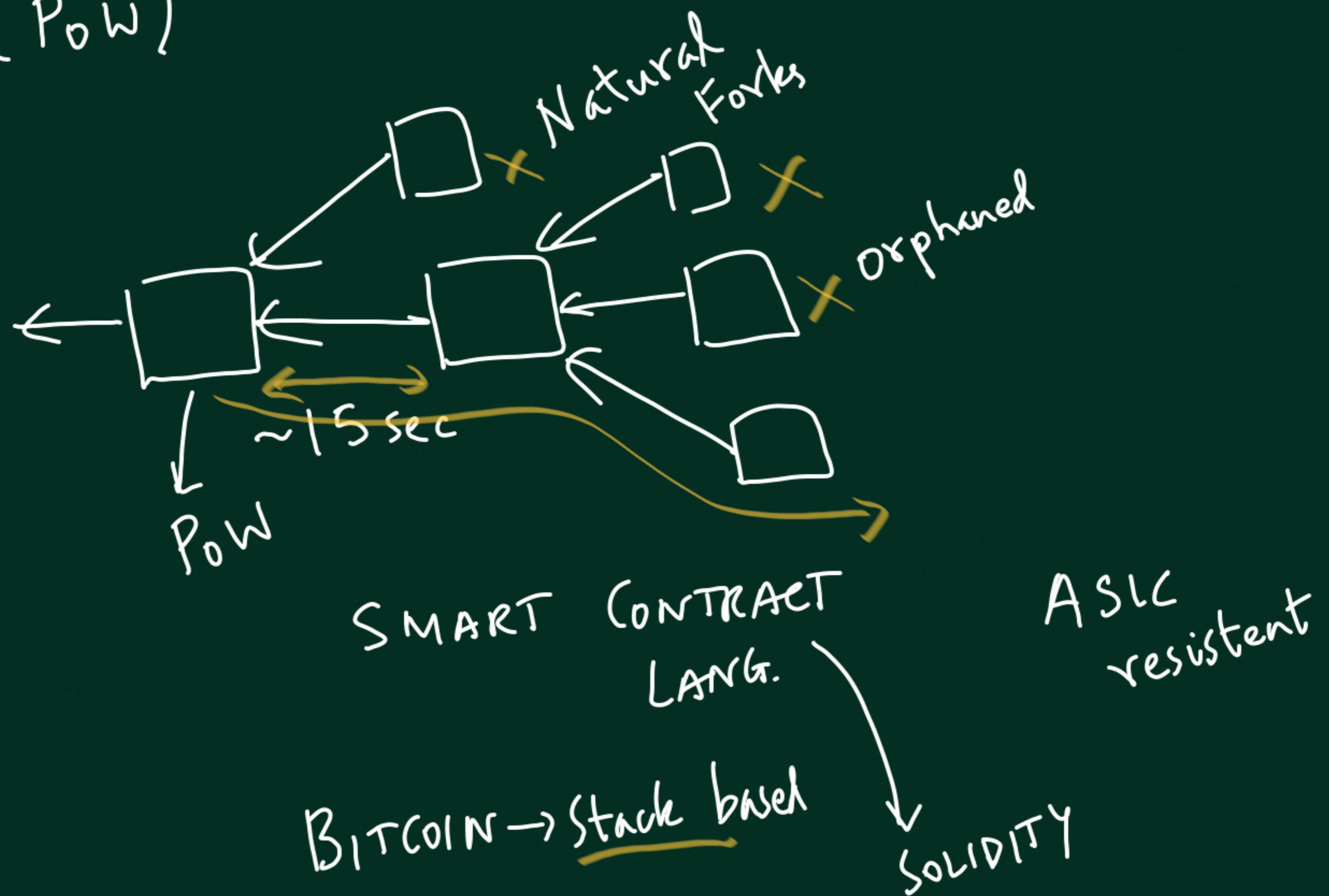


2014



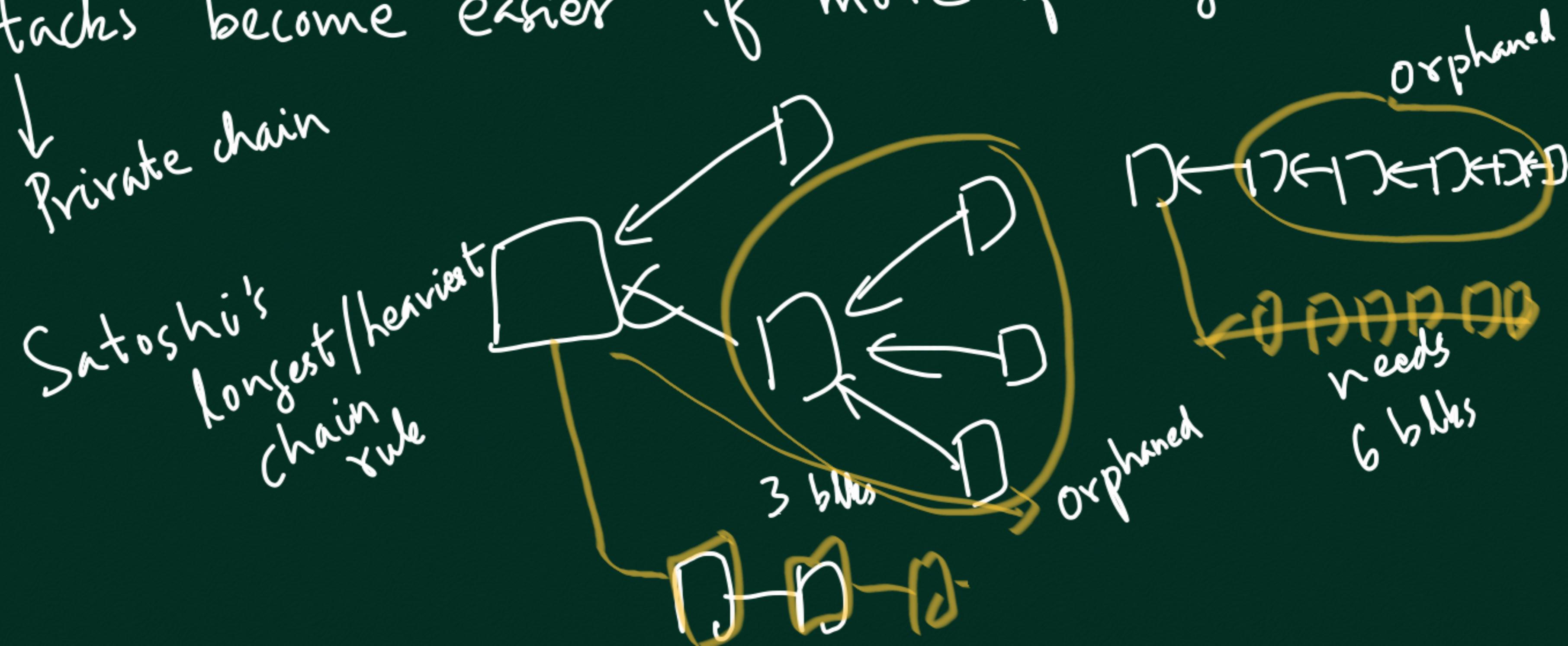
Attendance

Eth 1.0 (PoW)

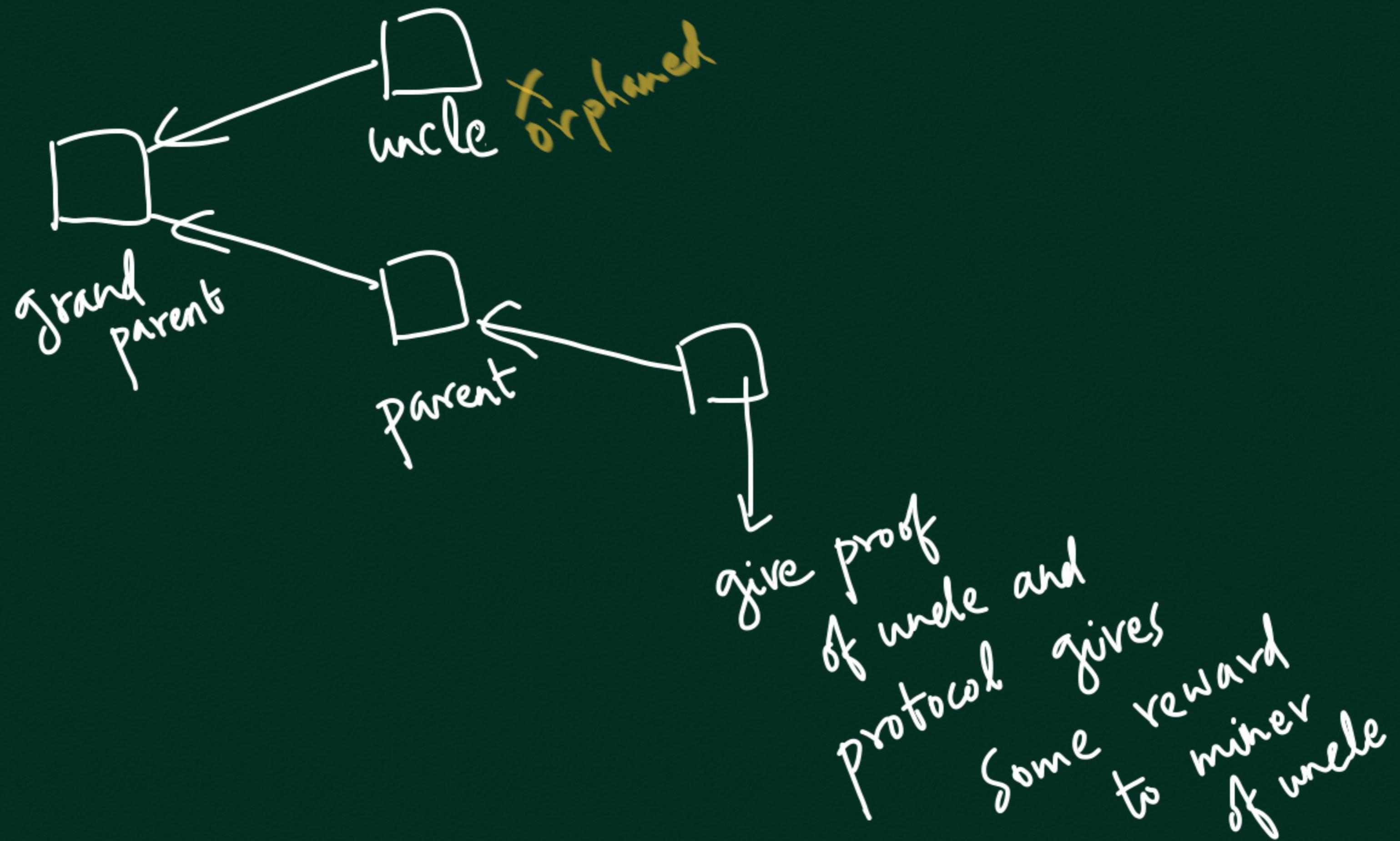


Issues

1. Too many blks orphaned → how to incentivize miners who may mine orphaned blks
2. Attacks become easier if more forking occurs

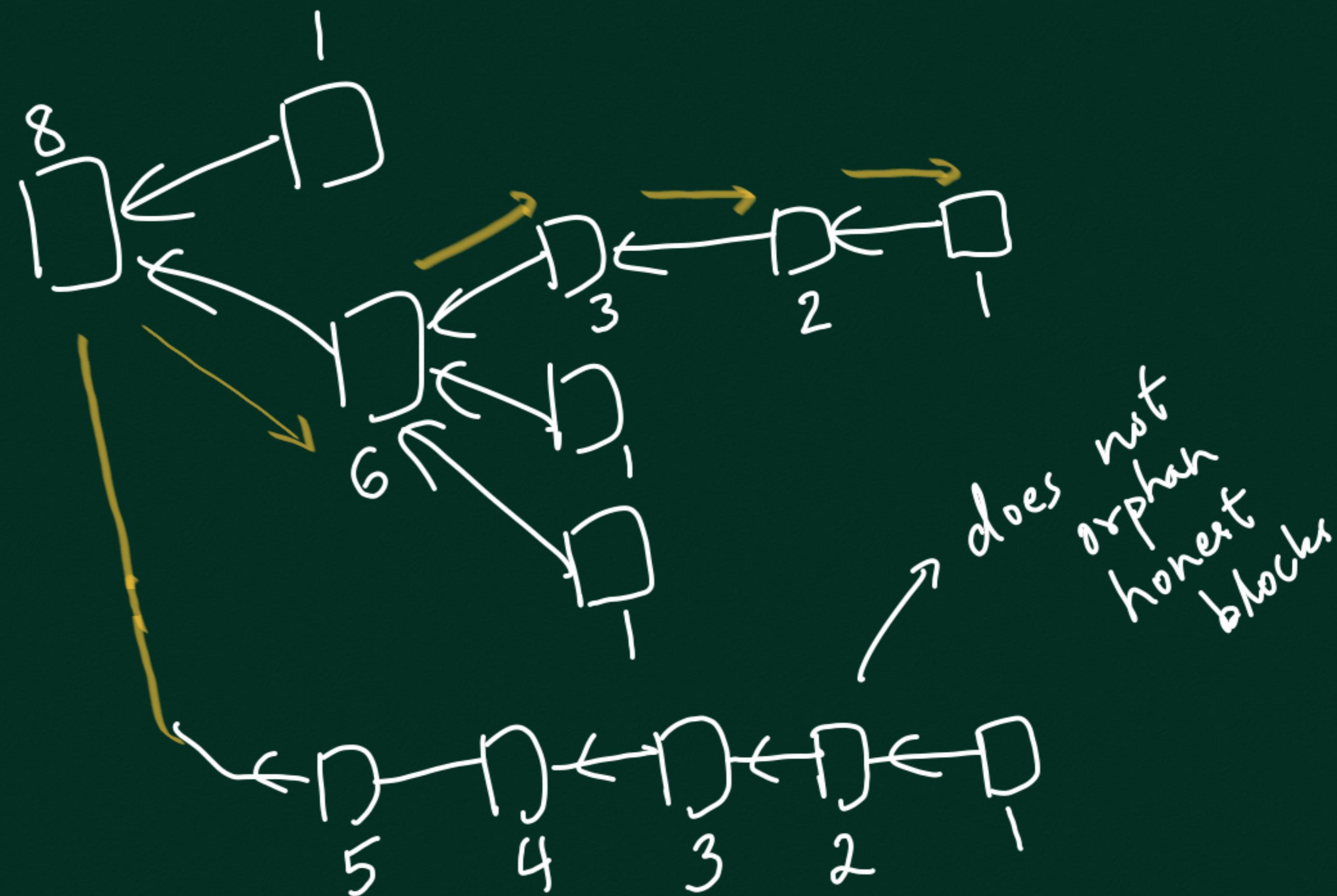


Soln 1: UNCLE REWARDS

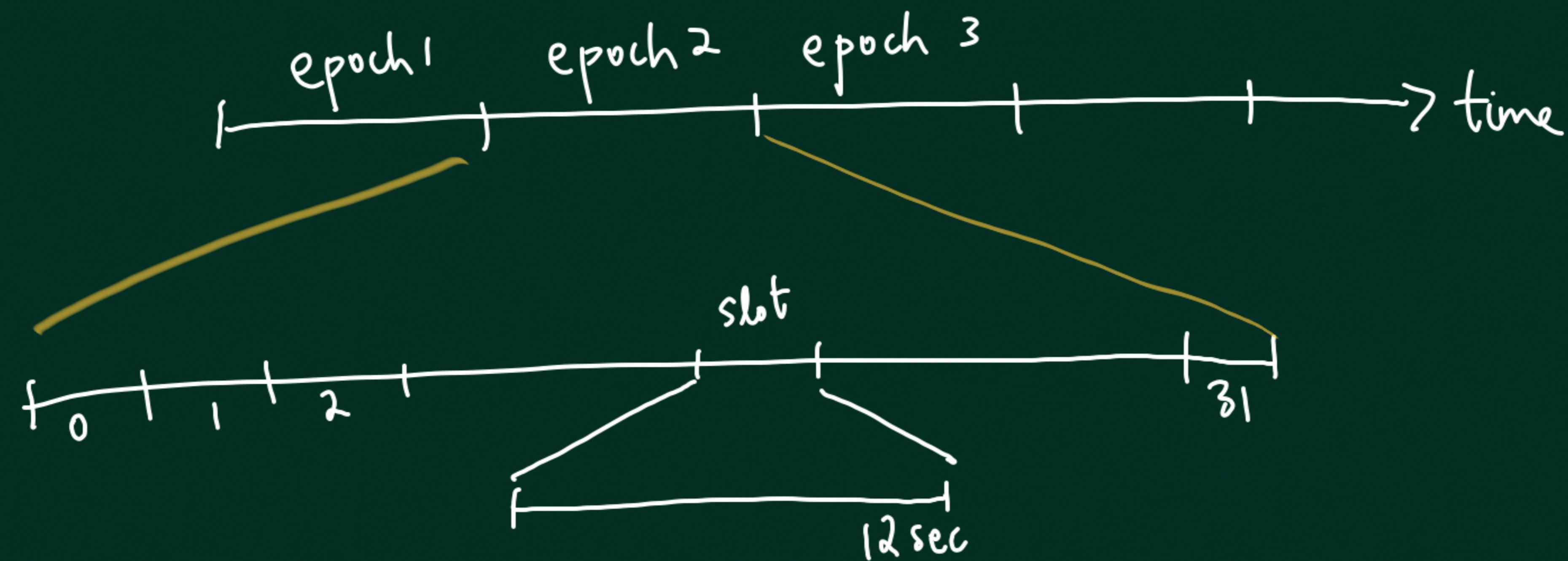


Soln 2: GHOST

Greedy Heaviest Observed Sub-tree

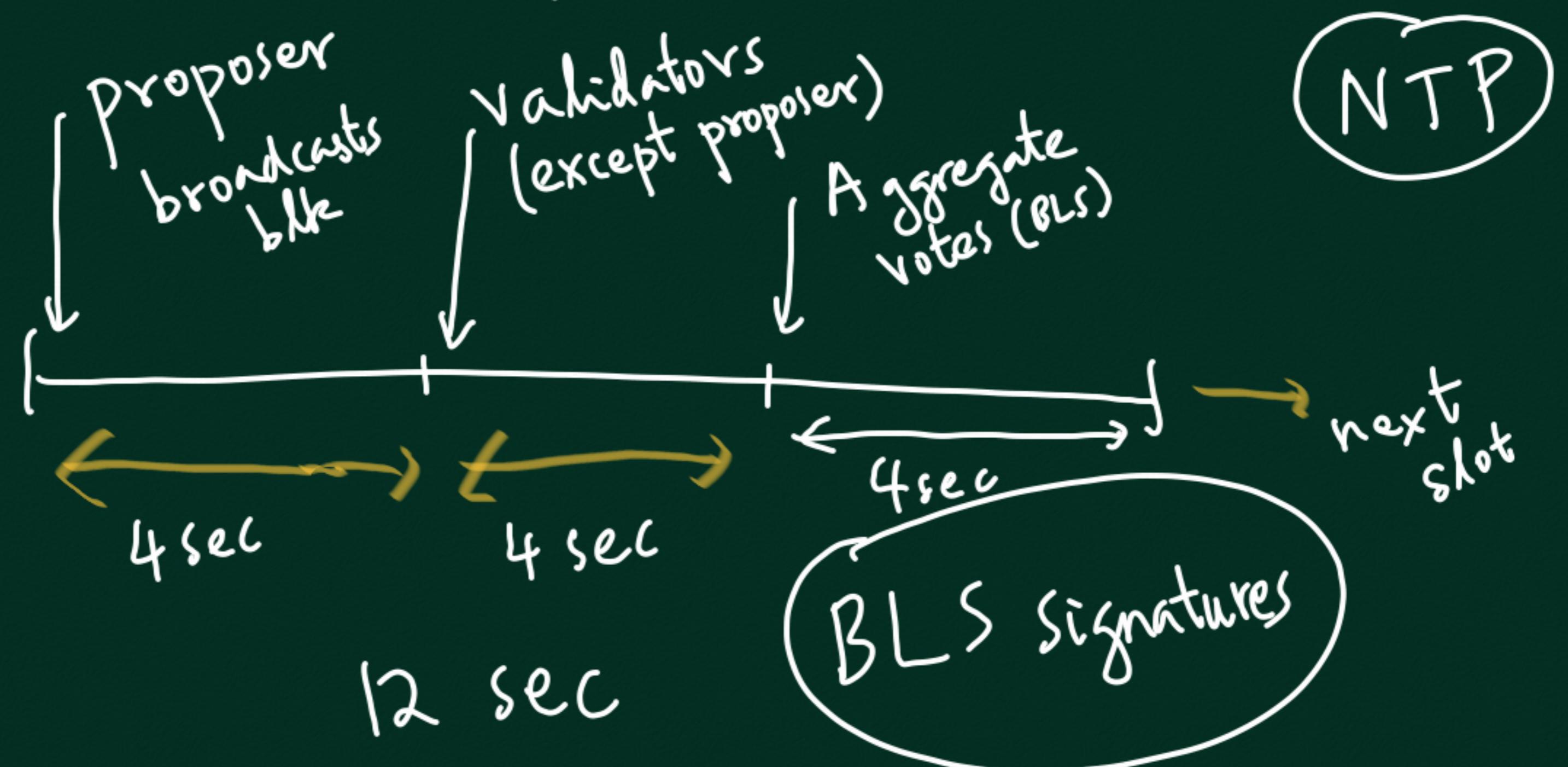


Eth 2.0: Pure PoS



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

Size \approx 1000's

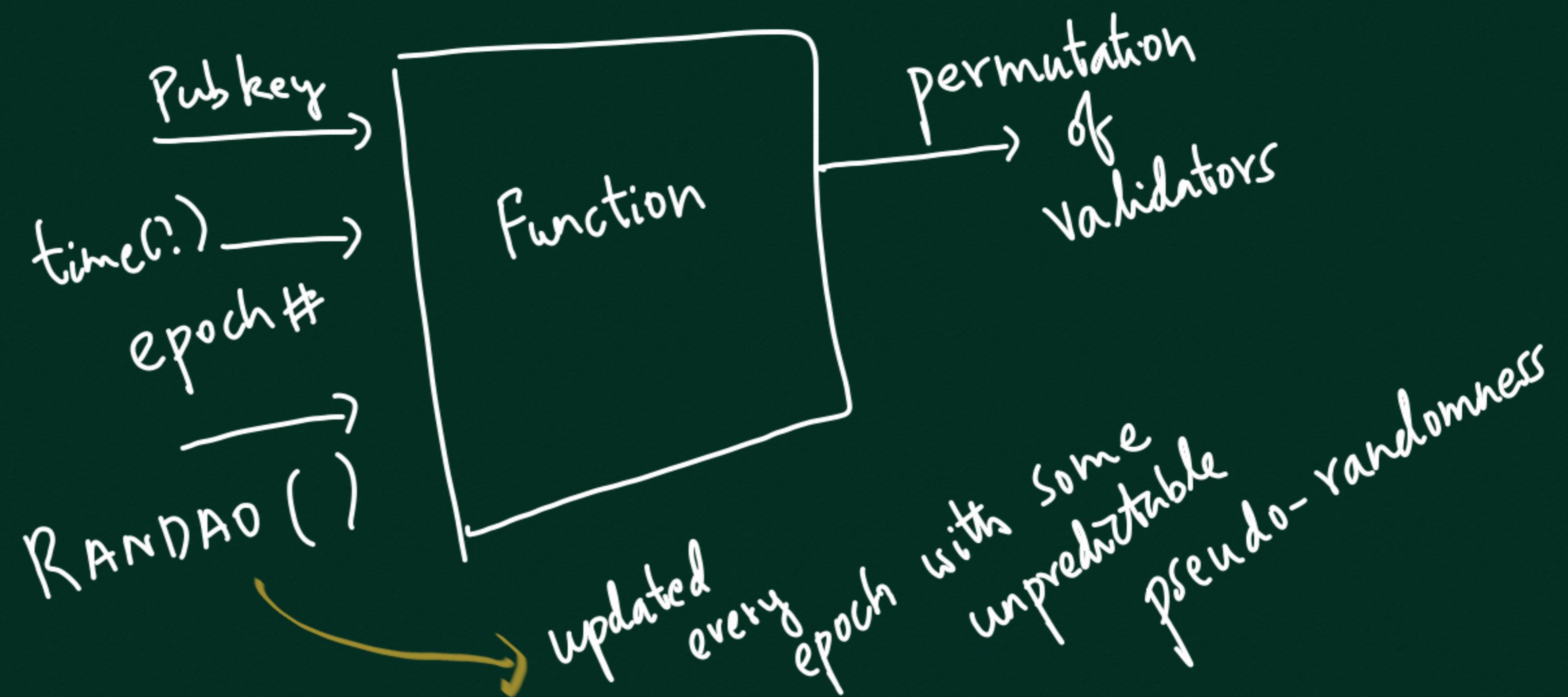


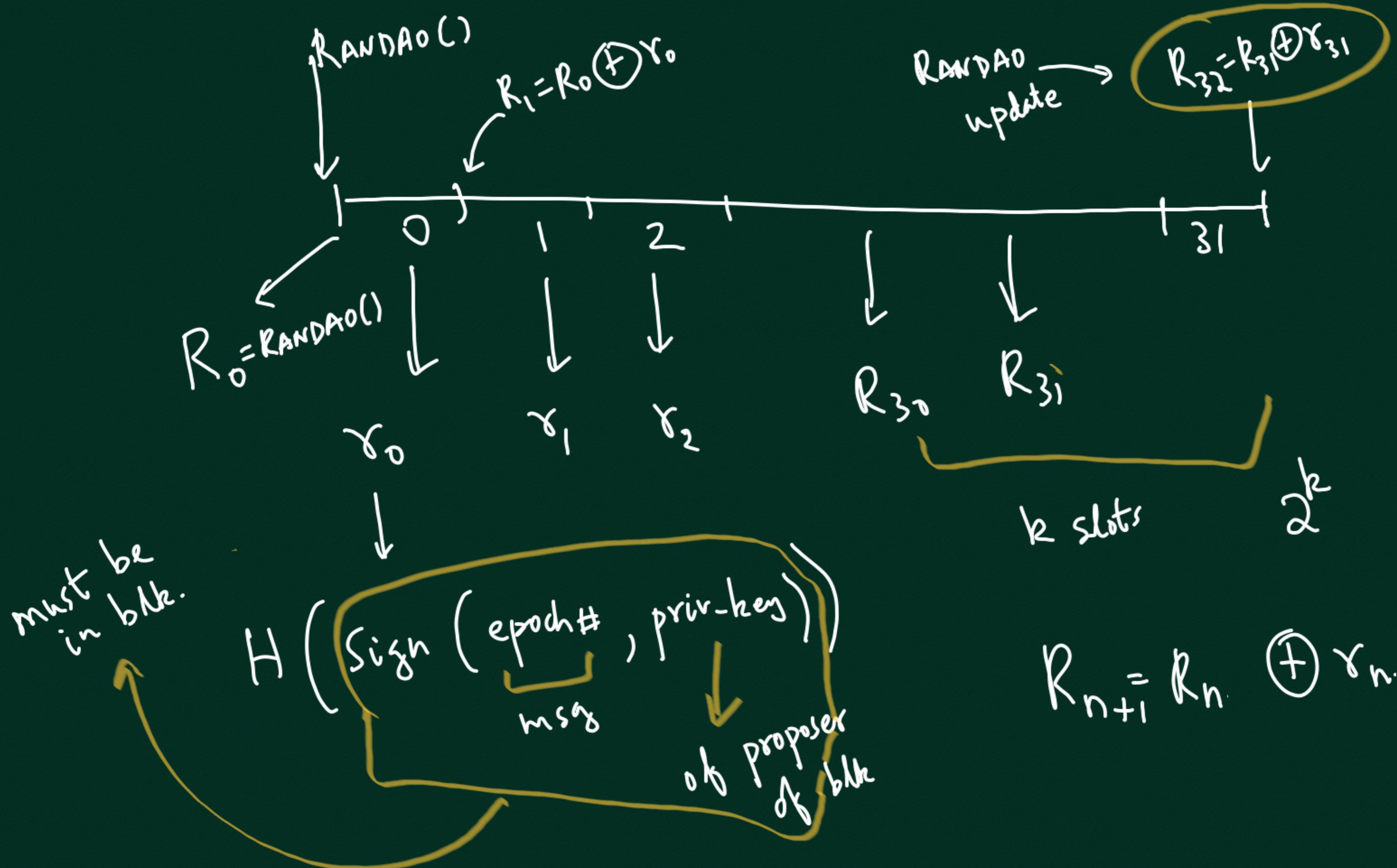
How to Select Committee?

- Deposit 32 ETH to become validator
- #.N^{10^5}
-
- The diagram illustrates the selection process. A large circle labeled "Validators" contains several smaller circles representing individual validators. Arrows point from these validators to three specific ones labeled C_0 , C_1 , and C_2 . These three validators are grouped together and labeled "Committee for slot -1". Below this group, a horizontal line represents a timeline with tick marks labeled 0, 1, 2, ..., 31, 32. Brackets indicate that each validator is assigned to one committee in an epoch, and that there are 32 committees in total across the slots.
- handle SYBIL
- can be SLASHED
- each validator assigned to 1 epoch
- Committee in an epoch
- 0 1 2 ... 31 32
- C_0 C_1 C_2
- Committee for slot -1
- gen. multiple blks in single slot
- Vote for multiple blks in same slot

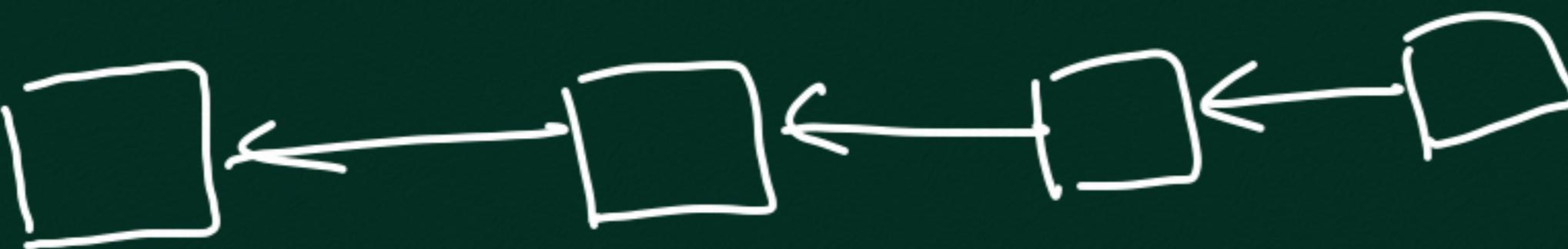
Randomness (?)

Validator: Pubkey, Privkey, Stake
↓
 $\approx 32 \text{ ETH}$



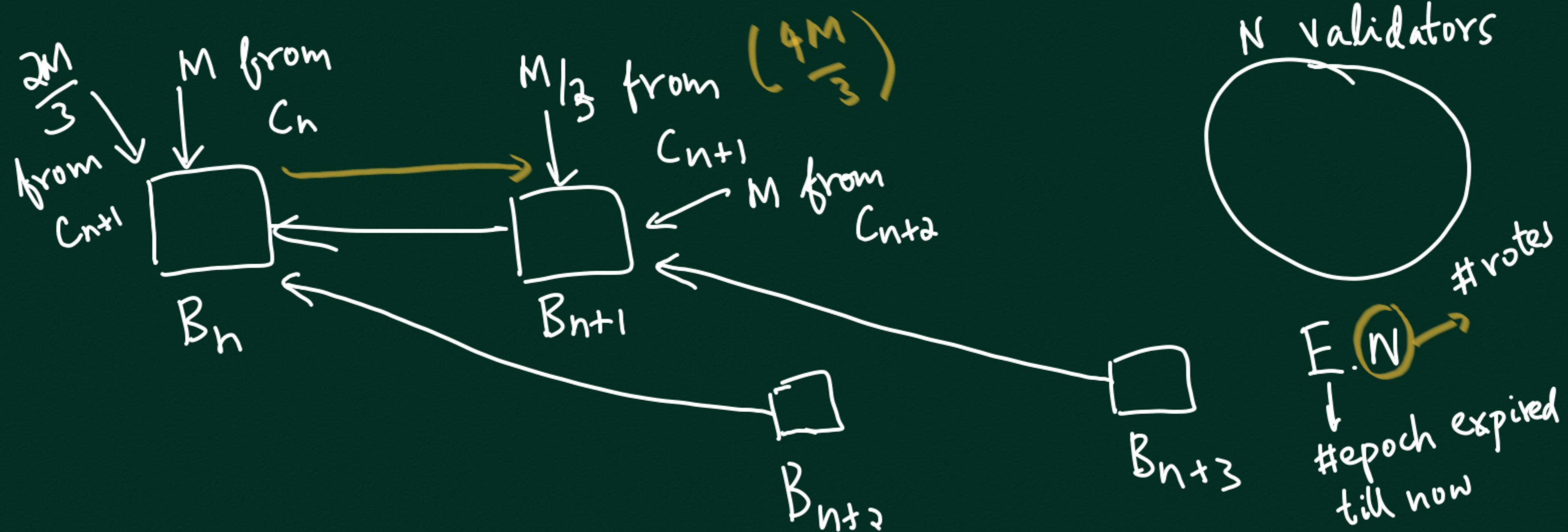


all honest,
net. delay < 4s



The diagram illustrates a sequence of blocks B_n , B_{n+1} , B_{n+2} , and B_{n+3} across three slots. The nodes are labeled C_n , C_{n+1} , and C_{n+2} . The diagram shows the following components and annotations:

- Block B_n :** Represented by a box containing the number n .
- Block B_{n+1} :** Represented by a box containing the number $n+1$.
- Block B_{n+2} :** Represented by a box containing the number $n+2$.
- Block B_{n+3} :** Represented by a box containing the number $n+3$.
- Miner:** A node connected to the blocks.
- Network Delay:** An annotation $\frac{M}{3} + \frac{2M}{3}$ with a yellow arrow pointing to the transition from B_n to B_{n+1} .
- Voter Sets:**
 - Set C_n : Contains M nodes.
 - Set C_{n+1} : Contains M nodes.
 - Set C_{n+2} : Contains M nodes.
 - Set C_{n+3} : Contains M nodes.
- Miner's Behavior:**
 - Miner sees B_{n+1} when his slot started.
 - Miner didn't see B_{n+1} when his slot started.
 - All M nodes voted here.
- Annotations:**
 - A yellow circle highlights the text "M nodes & C_{n+2} ".
 - A yellow oval highlights the text "miner didn't see B_{n+1} when his slot started".
 - A yellow bracket groups B_{n+1} and B_{n+2} .
 - A yellow bracket groups B_{n+1} and B_{n+3} .
 - A yellow bracket groups B_{n+2} and B_{n+3} .
 - A yellow bracket groups B_{n+1} , B_{n+2} , and B_{n+3} .
 - A yellow bracket groups C_n , C_{n+1} , and C_{n+2} .
 - A yellow bracket groups C_{n+1} and C_{n+2} .
 - A yellow bracket groups C_{n+2} and C_{n+3} .
 - A yellow bracket groups C_n , C_{n+1} , and C_{n+3} .
- Text Annotations:**
 - "net. delay is large"
 - "How to deal with forks?"
 - "(let's use GHOST)"
 - "Use GHOST to vote for B_{n+1} "
 - "Use GHOST to vote for B_{n+2} "
 - "all see B_{n+1} and B_{n+2} "
 - "suppose all see B_{n+1} and B_{n+2} "
 - "Do S"



LMD-GHOST

Latest Message Driver

(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)

