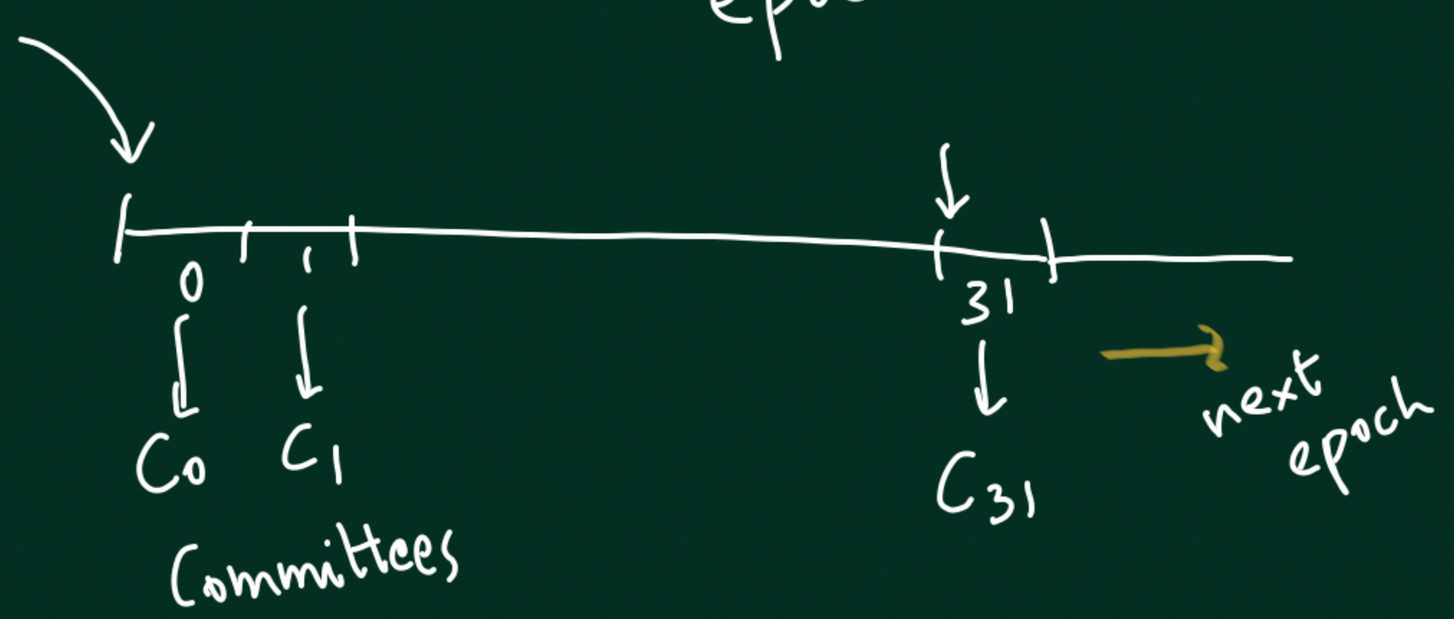
Eth 2.0: Pure PoS

(Book) online ethatools..... → Moodle

GHOST + SLASHER + ...

epoch → 32ETH



Attendance

Next class: Oct 22 (Wed)
8:30, in KR125

- Each committee member votes for blocks

Two types of votes

(1) Voting for tip of chain (to say what is current valid chain)

→ LMD-GHOST vote

(2) Voting to finalize blocks

→ CASPER - FFG

Friendly finality Gadget

In PoW, no FINALIZATION, any blk can be orphaned

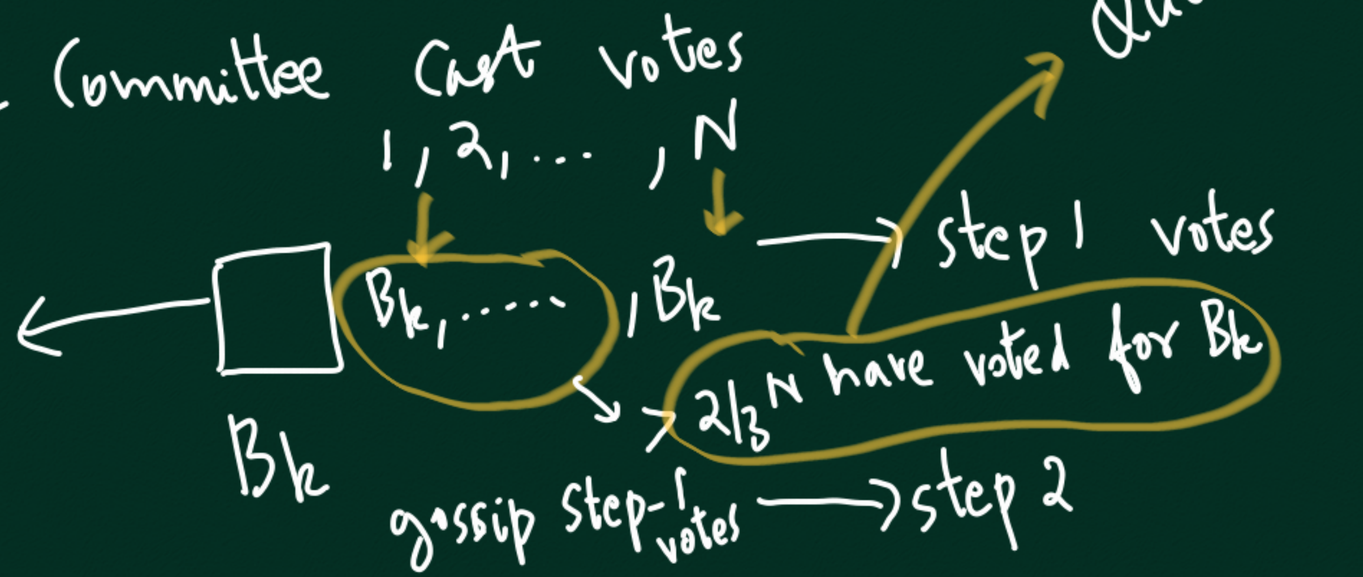
PoS ⟶ BFT ideas

N participant in consensus

PBFT

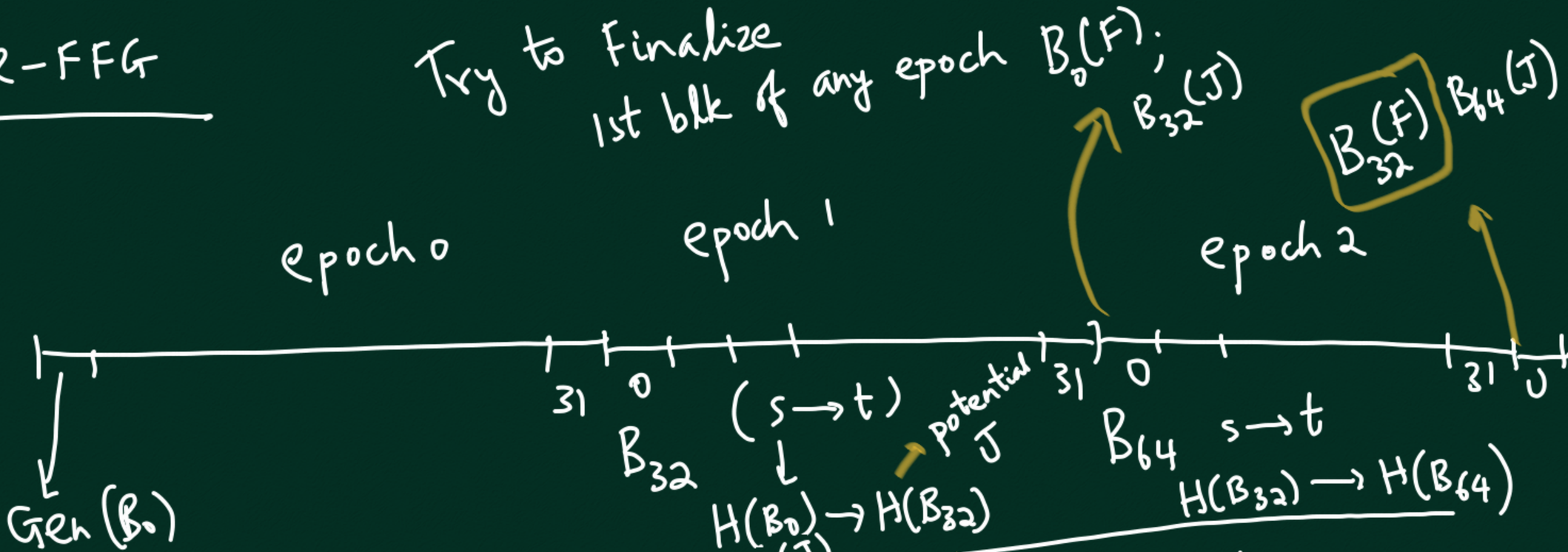
$< \frac{N}{3}$ are malicious, rest honest

High Level: Single Committee Cast votes



CASPER-FFG

Try to Finalize
1st blk of any epoch



Initial: Gen is Justified AND FINALIZED

Vote: $s \to t$ (hash)
- s: hash of last J blk
- t: my vote for next J blk

Justified (J) → if validator hears $> \frac{2N}{3}$ Saying want a blk

Finalized (F)
- if $> \frac{2N}{3}$ say they heard $> \frac{2N}{3}$ accepted a blk to be justified
- Justified like Step-1 of BFT protocol

LMD-GHOST

A validator does in every slot

(1) Run CASPER-FFG, it returns highest J block

* Note: Use votes already in blockchain

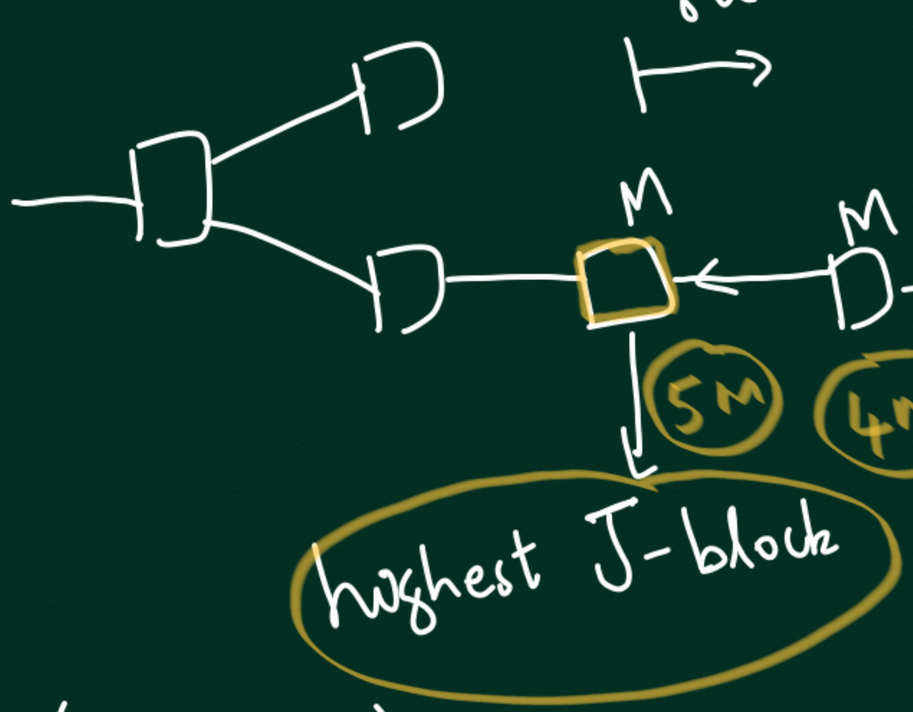
(2) Start from this J-block and run LMD-GHOST

* Use all votes heard (not necessarily included in blockchain),

provided these were cast in prev. slots

s → t

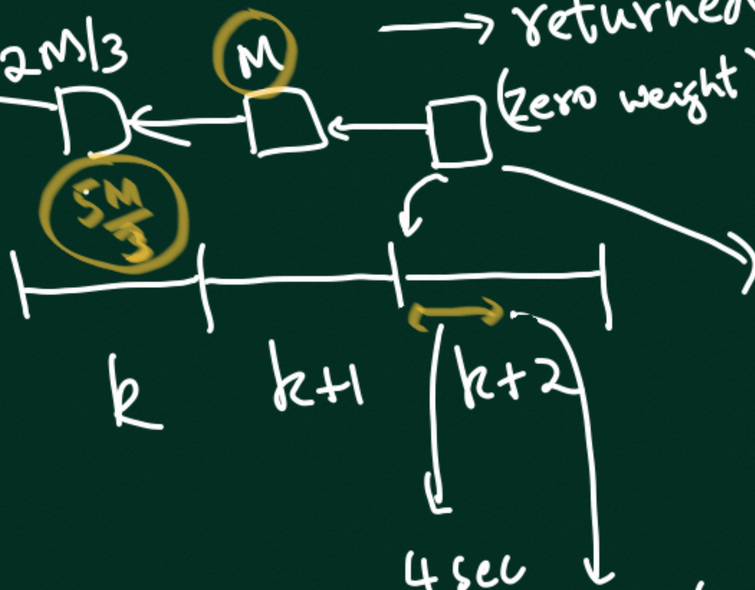
run LMD-GHOST



Case (i)

Miner (validator) supposed to mine in slot k+2

→ returned by LMD-GHOST (zero weight)



created by this miner

Note: (LMD-GHOST)

In case of tie, use higher blk hash to proceed.

$|C| = M$

$M = \frac{N}{32}$ → total validators

Case (ii) Voting miner in slot (k+2)

Runs LMD-GHOST, votes for tip of chain

RE-ORG Attack

attacker as Proposer

B_n

B_{n+1} (1)

vote

honest proposer

B_{n+2} (0)

0

4 sec

B_{n+3}

$|C| = 8$

LMD-GHOST votes

8+7 (at start of n+2 slot)

attacker

keep B_{n+1} and single vote hidden

gets orphaned

(n+2)

attacker releases B_{n+1} and single hidden vote

LMD: Latest Message driven

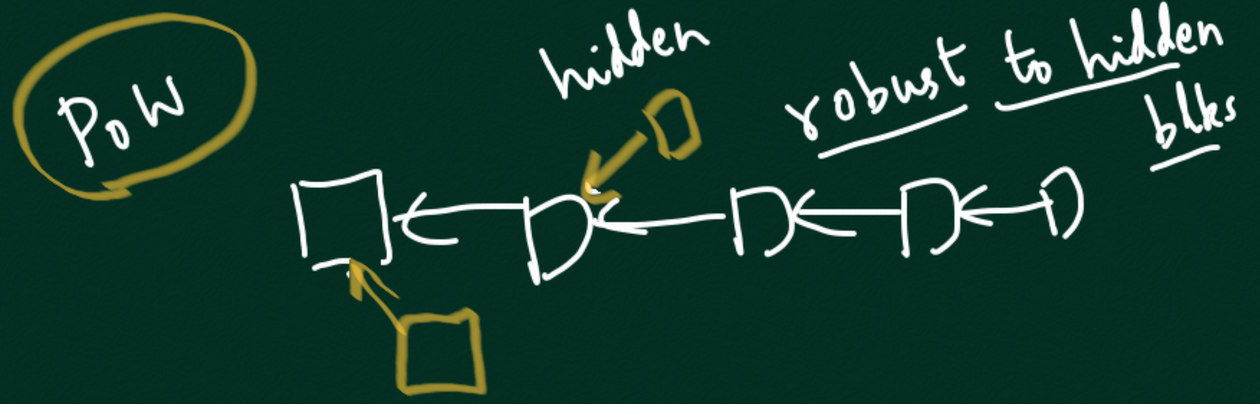
Handles 2 issues with GHOST

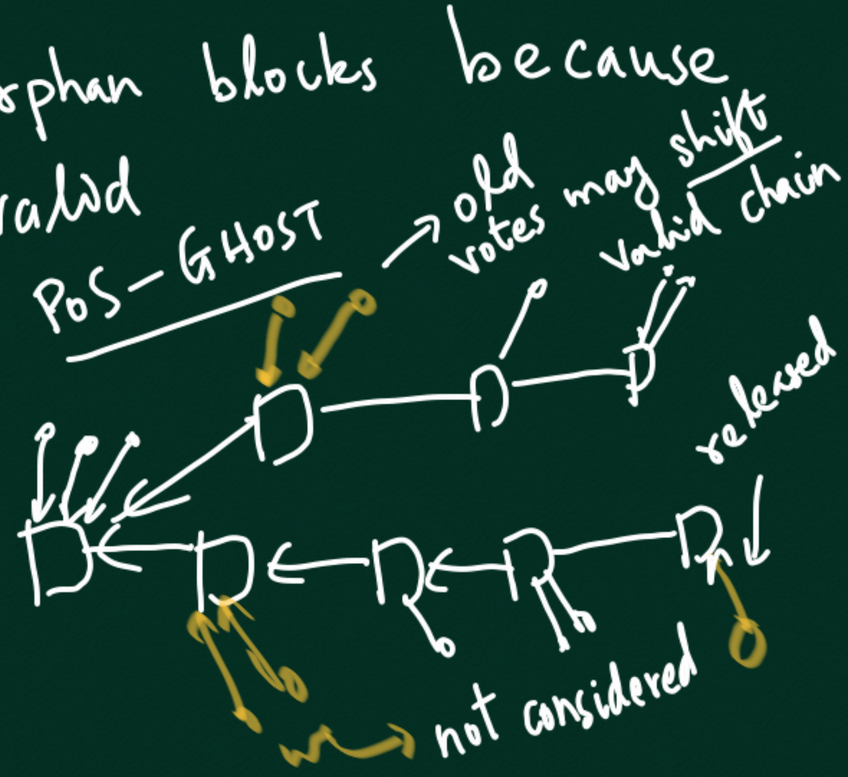
(1) Too many votes: E epochs, N validators

ExN (normal GHOST)

N votes (LMD-GHOST)

(2) Very old votes can potentially orphan blocks because they are always valid





Quiz

M v X C Q V B A