PBFT: Castro & Liskov (1999)

Attendance

$N = 3f + 1$

f → max. Byz. Nodes

Quorum: $2f+1$ nodes agree

Inters. Property

Availability

Log

index ... n

entry/msg ... m

view v

term in RAFT

Primary $\langle n, m, v \rangle \rightarrow$ node

$\langle n, m', v \rangle \rightarrow$ another node

$m' \neq m$

Everyone has Pub/Sec. key pair, unknown to others

$\langle$ message $\rangle_\sigma$

$\sigma \rightarrow$ signature

Forging sign not possible

client → Primary

Node-2

Node-3

$m = \langle REQ, o, t, c \rangle_{\sigma_c}$

Operation

ID of client

timestamp

should increase for every new message

⋮

Node-N

Honest Primary (Log)

index

entry

view

n

m

v

PRE-PREPARE

PREPARE

$\langle PRE\text{-}PREPARE, v, n, m \rangle_{\sigma_p}$

PRE-PREPARE Phase: On receiving $\langle v, n, m \rangle$ from Primary

if node$^{(i)}$ is in view v, and has not accepted another message in view v for same 'n',

then it puts $\begin{pmatrix} n \\ m \\ v \end{pmatrix}$ in its log, and sends

out $\langle \text{PREPARE}, v, n, m, i \rangle_{\sigma_i}$ in next phase

Note: Honest node sending $\langle \text{PREPARE}, v, n, m \rangle_{\sigma}$ will not send $\langle \text{PREPARE}, v, n, m' \rangle_{\sigma}$ $m' \neq m$

PREPARE Phase: If node-i has sent $\langle \text{PREPARE}, v, n, m \rangle_{\sigma_i}$

and it hears 2f or more other nodes sending PREPARE with same tuple (v, n, m) then we say it has P_CERTIFICATE for (v, n, m)

Note: If a node (honest) gets P-CERT for (v, n, m); then it is SURE that no one else can get P-CERT for (v, n, m') where $m' \neq m$

(Using Inters. Prop. of Quorums)

Honest

Log

index . . . n

entry/msg — m

view —.. v

LOCKED

P-CERT

have if ∧ P-CERT for (v, n, m)

then don't accept or send PREPARE for this tuple

Suppose view-change occurs (e.g. $v' = v+1$)

Suppose Primary send (v', n, m')

where $m' \neq m$

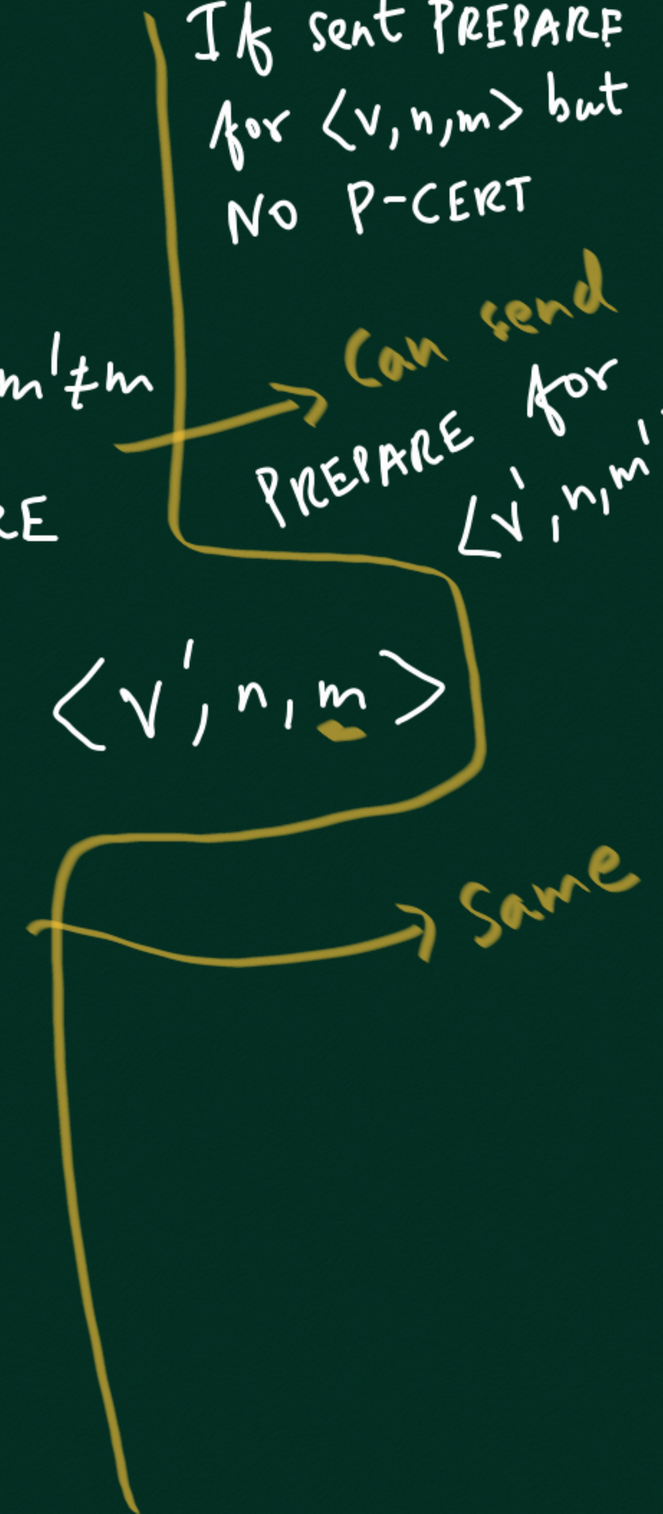
If have P-CERT for $\langle v, n, m \rangle$

- Get PRE-PREPARE in $v' > v$ for $\langle v', n, m' \rangle$, $m' \neq m$

  don't accept or send PREPARE

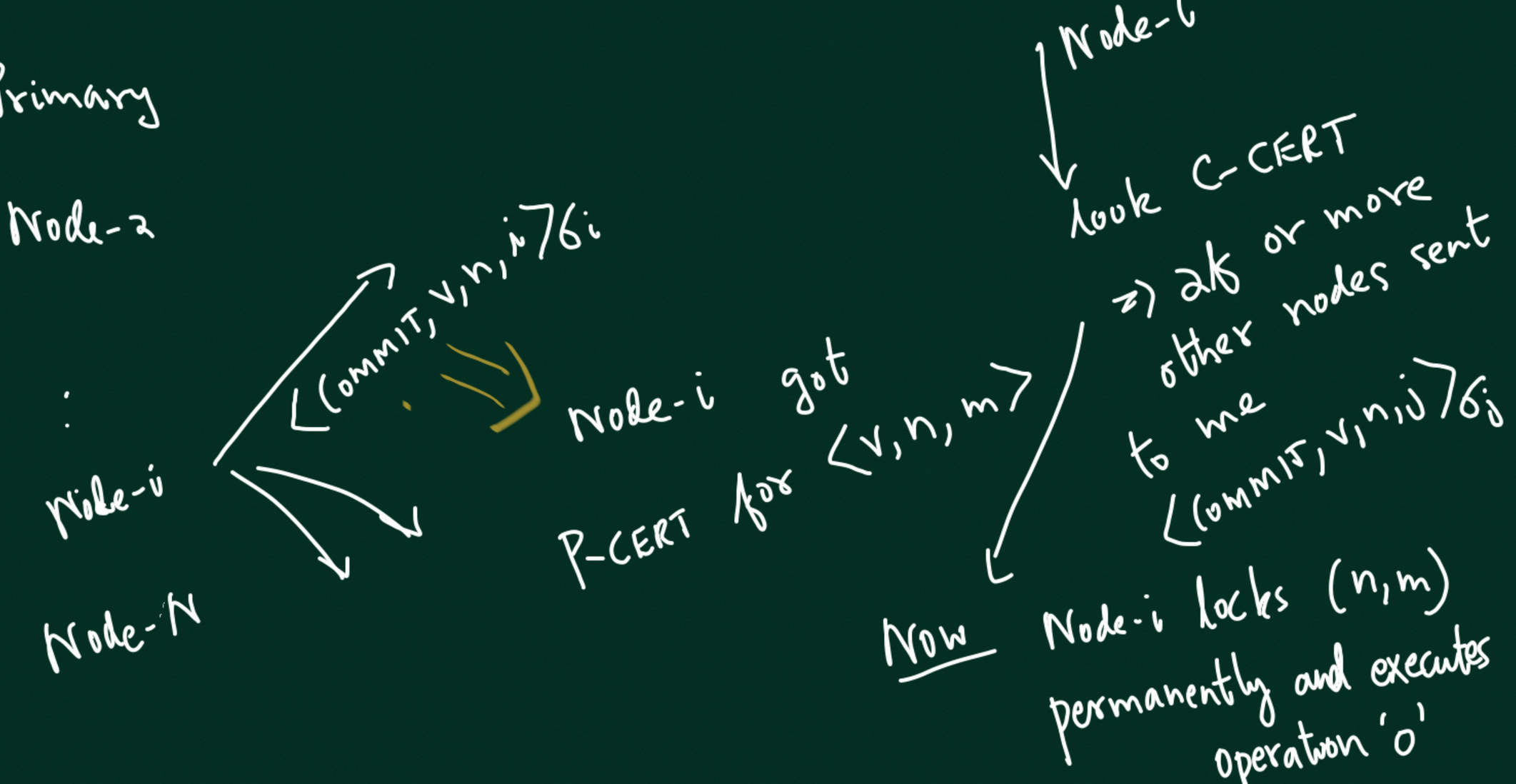
- Get PRE-PREPARE in $v' > v$ for $\langle v', n, m \rangle$

  then send PREPARE for $\langle v', n, m \rangle$



PREPARE phase ensures total ordering within a view

COMMIT Phase: Gossip if P-CERT heard in previous phase



If C-CERT obtained, then 2f+1 nodes have received P-CERT for (v, n, m) and will not vote (PREPARE) for (v', n, m') where $v' > v$, $m' \neq m$

Reply phase: