All committe members propose blocks

B_1
B_2
$\vdots$
B_N

B' or Empty

All honest say either B' or Empty

step-1 | step-1 / Step-2 | (step-1,2,3)(4,5,6)(7,8,9)

Phase-0 | Phase-1 | Binary BA*

Block Proposal | Reduction | Phase-2

BA*

$j > 0 \Rightarrow$ am in committe

$(0, 2^{hashlen} - 1)$ pseudo-rand# distrib.

(want

(hash, π, j) π proof

VRF$_{sk}$(seed||role)

PBFT

depends on phase, step# etc.

Attendance

SORTITION

w, W

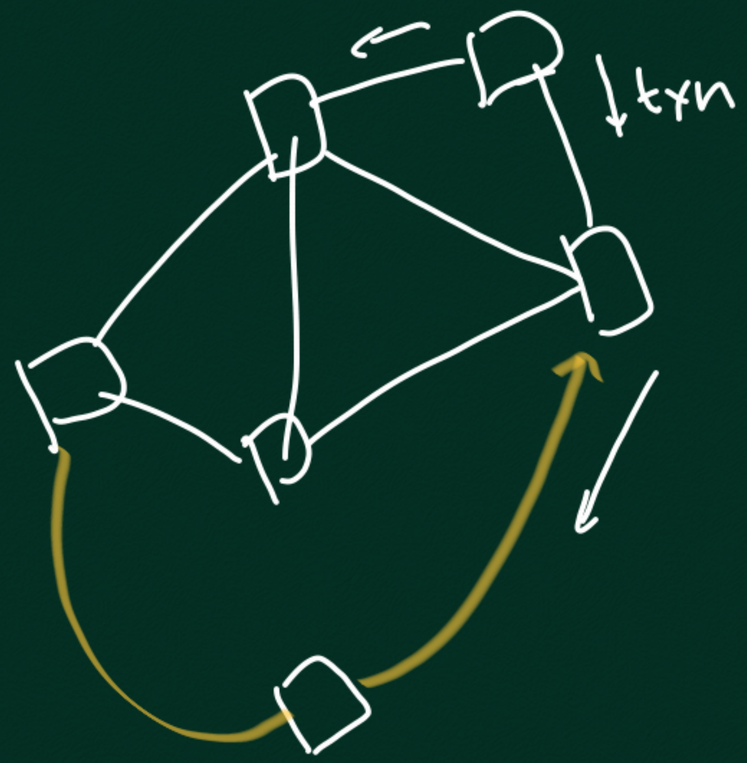
#tokens (pk,sk) has

total # token

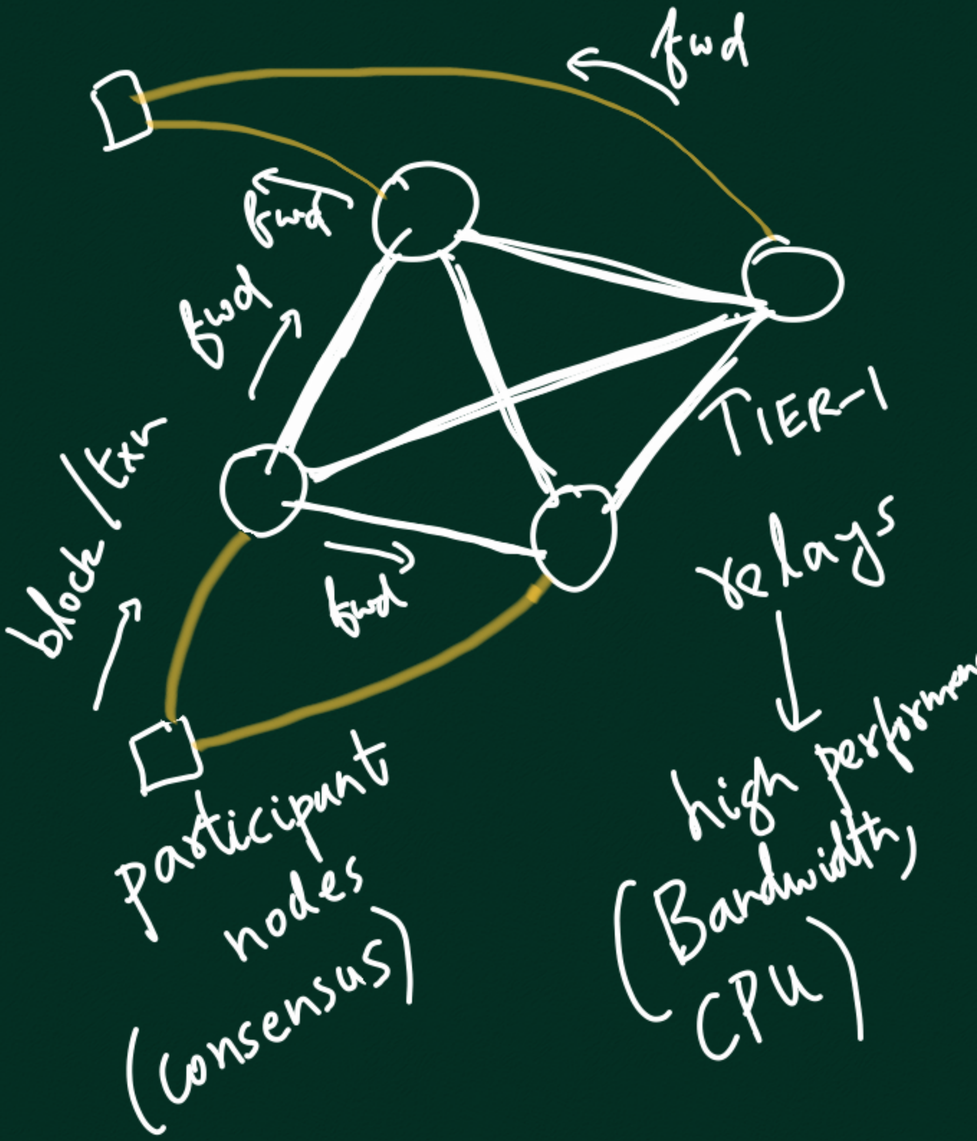
small 'w'

B(k; w, p)

BITCOIN NETWORK



ALGORAND

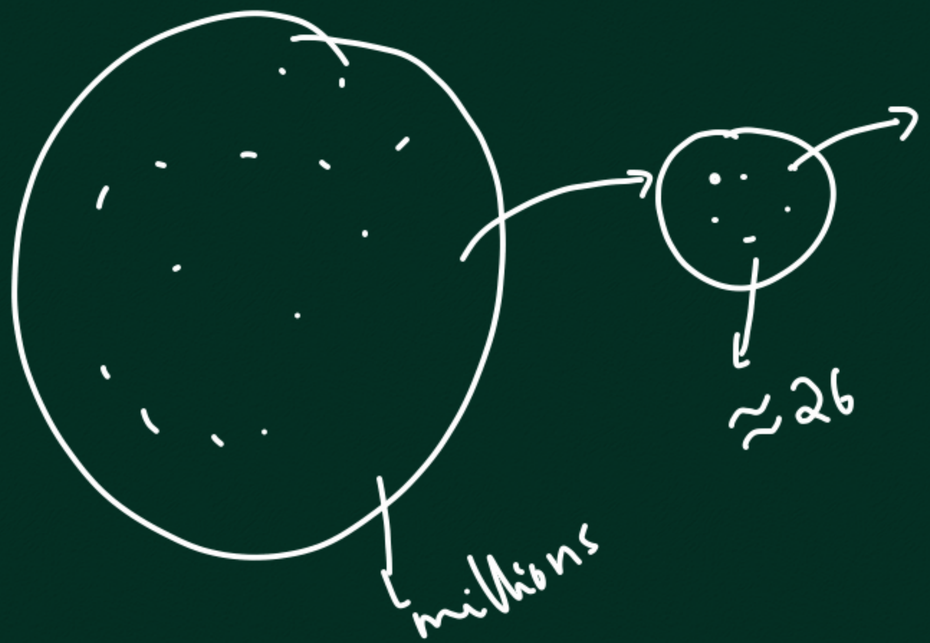


Phase-0

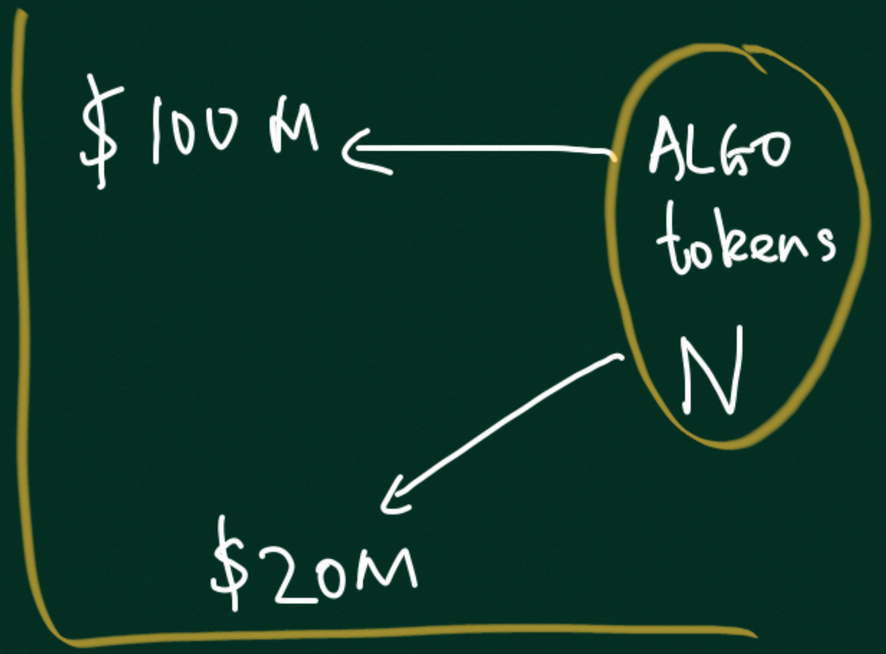
$\tau_{PROPOSER} = 26$

↓

Expt. Committee size



85%



Priority of one user

$\max H(hash \,||\, i)$

$i = 1, 2, \ldots j$

↓

#subuser

Choose Highest Priority member, If multiple blks from this member, tie-break via blk hash. Lowest(?)

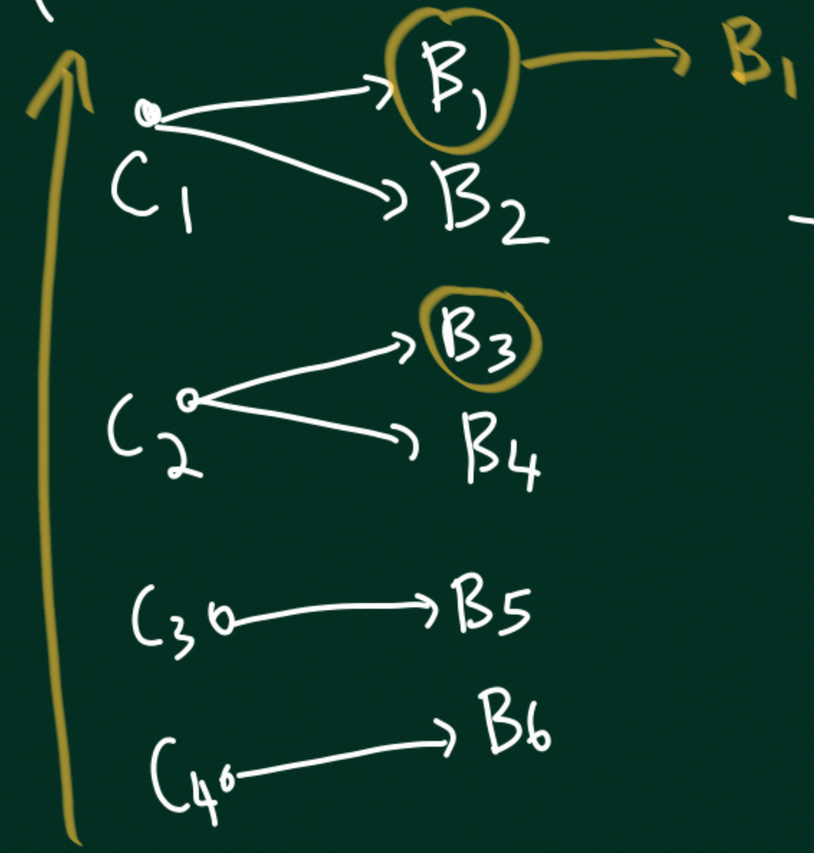
$\langle hash, \pi, j \rangle$

↓

output of SORTITION

Phase-0

Priority



Honest

X — Y (not seen B_1) — Z (not heard from C_1)

B_2 B_3

↓ Input

Reduction

Reduction

Step-1

only Committee members { Announce block from Phase-0,

Everyone → Count # votes for each block

If Quorum for particular block
set $r \leftarrow$ (that blk.)

If Timeout (no quorum)
$r \leftarrow$ Empty

Step-2

Vote (r) ⟶ Selected members

Count votes

If Quorum, set r ← that block

If Timeout then r ← empty

What might happen, AFTER reduction

X → B_1

Y → B_1

Z → empty

τ (committee size) If T fraction of committe votes for a block, we say we have "Quorum"

$T_{Reduction} = 2000$

$T_{reduction} = 0.685$

BINARY BA*

(3k+1) (3k+2)

input B_1 or $\emptyset$

step-1 → step-2

look for Quorum;
if Quorum for B_1 vote for it for next 3 steps (and ....)

if Quorum (B_1) then vote B_1 in next step (provided no conflicting candidate)

Consensus on B_1

if Quorum for empty vote for it next

Don't declare consensus on Empty

else (Timeout) prefer B_1 (vote B_1 in next step)

Hear Quorum for EMPTY

else (TIMEOUT) prefer EMPTY (vote Empty in next step)

Consensus for Empty (vote Empty, next 3 steps)

(3k+3)

Step-3 .. — Steps-4-5-6

↓ ↓ ↓

1 2 3

if

Quorum for B_1

vote for B_1 next

(assuming no consensus earlier)

if Quorum for Empty

vote Empty next

Timeout case: Use CommonCoin

to vote next

if CommonCoin = 0, vote B_1

= 1, vote Empty

Common Coin

User-k in committee in step-3

$\langle hash_k, \pi_k, j_k \rangle$

$n_k = \min_{i=1,\cdots,j_k} H(hash \| i)$

$LSB\left(\min_k n_k\right)$

↳ CommonCoin

Suppose attacker's n_k value is not the smallest, then all end with same CommonCoin