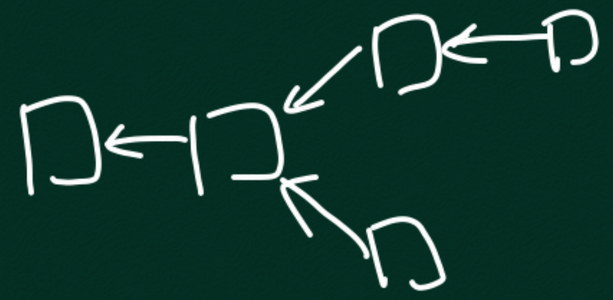
PoW, Naive PoS, SLASHER

Eth 2.0 → 2022, RAFT, PBFT

Attendance

ALGORAND – 2017



Silvio Micali (Turing Award)

Pure PoS ✓, No FORKS ×, CONFIRMATION TIME: 1 Minute

Decentralized ✓, Random Proposer ×, DoS robustness

#txns/sec ≈ 1000 >> Bitcoin's 7 txn/sec

Assume: ~85% of Stake Honest, Delay is few sec.

Stake and no forks

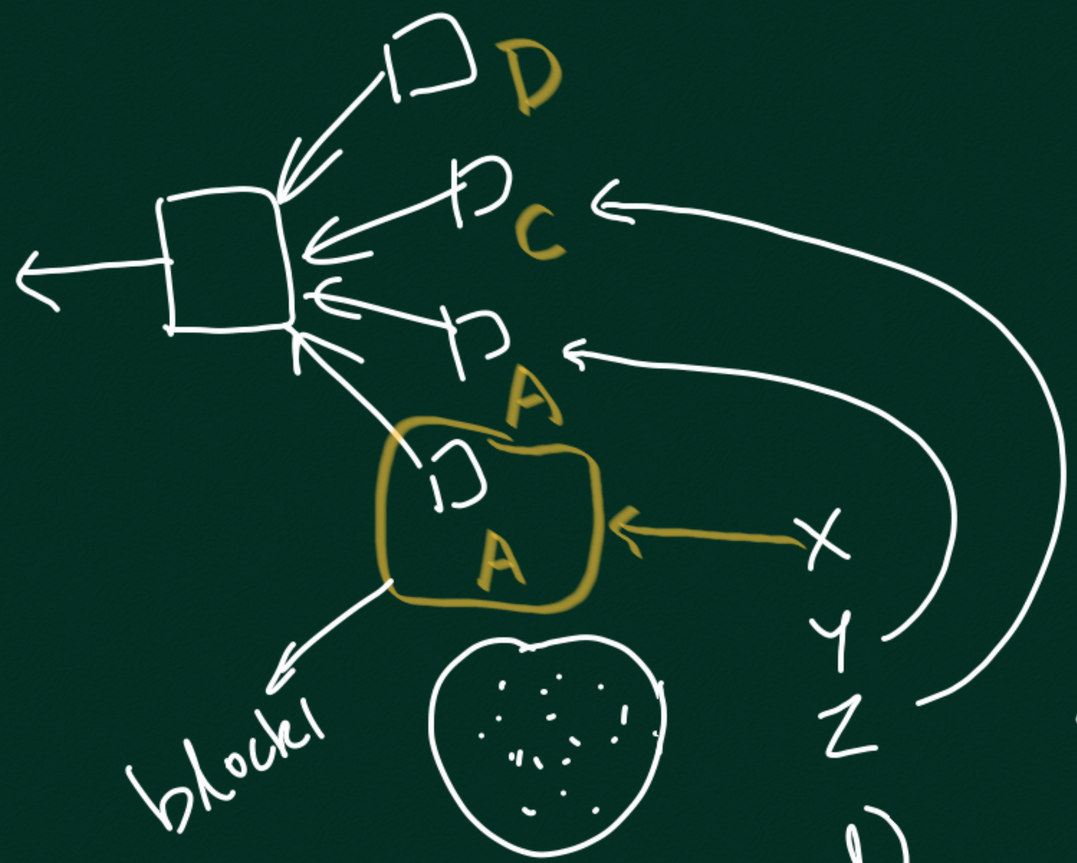
Stake & PBFT?

↳ only N nodes

acct bal(acct)

$H(\text{acct} \,||\, \ldots) \leq \text{target} * \text{bal(acct.)}$

High-Level Idea.

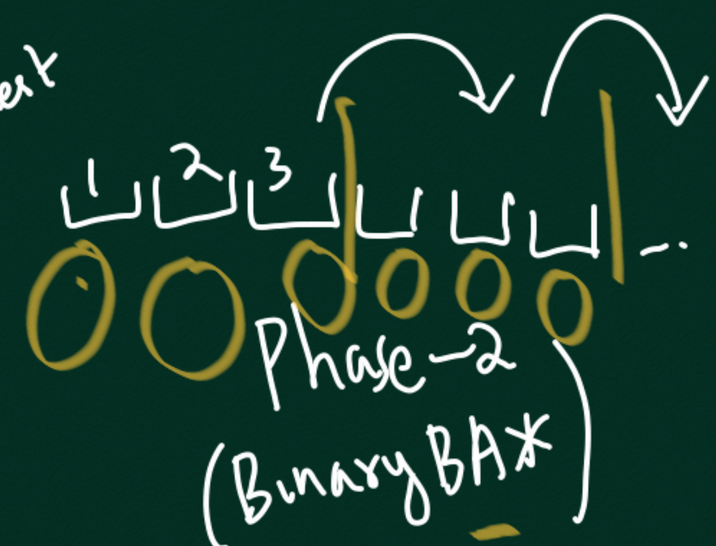


Guarantee

X → block1
Y → empty blk
Z → block1
C → block1
D → empty
E → block1

~ Honest

All Honest either block1 or empty



How to randomly form a DoS-resistent Committee

Sef-Select, prove later that selected

(VRF: Verifyable random function (Tool used)

→ (pk, sk)

key pair

⟨hash, π⟩ ← VRF$_{sk}$(x)

hash → pseudo-random value

π → proofs (that for your "hash" was so and so value

x → seed (input string)

msg $SIGN_{sk}(msg)$ $Verify(SIGN_{sk}(msg), msg, pk)$

Suppose: $hash = H(SIGN_{sk}(x))$ } example VRF

$\pi = SIGN_{sk}(x)$

$SORTITION(sk, seed, \tau, role, w, W)$

- τ → Expct. Size of committee
- role → changes from one step to another
- w → stake associated with (pk, sk)
- W → total stake

SORTITION (sk, seed, τ, role, w, W)

$\langle hash, \pi \rangle \leftarrow VRF_{sk}(seed \| role)$

$0 - \binom{hashlen}{2} - 1$

$p \leftarrow \frac{\tau}{W}$

unif → (Convert) → Binomial

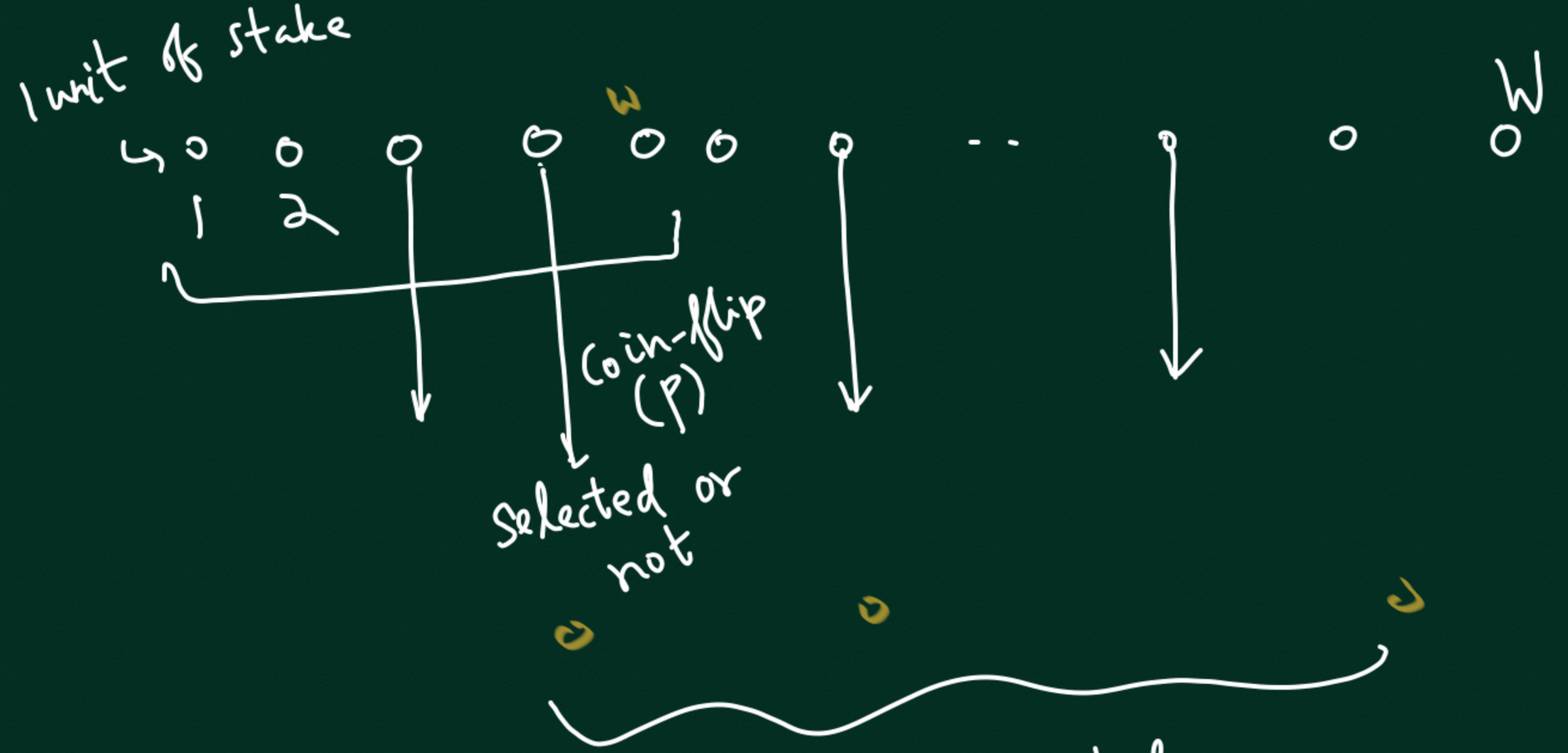
#times elected to committee (#sub-users)

$j \leftarrow 0$

while $\left(\frac{hash}{2^{hashlen}} \geq \sum_{k=0}^{j} B(k; w, p) \right)$

$j++;$

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


1 unit of stake
1
2
W
Coin-flip (P)
Selected or not
T selected on avg.

$p = T/W$

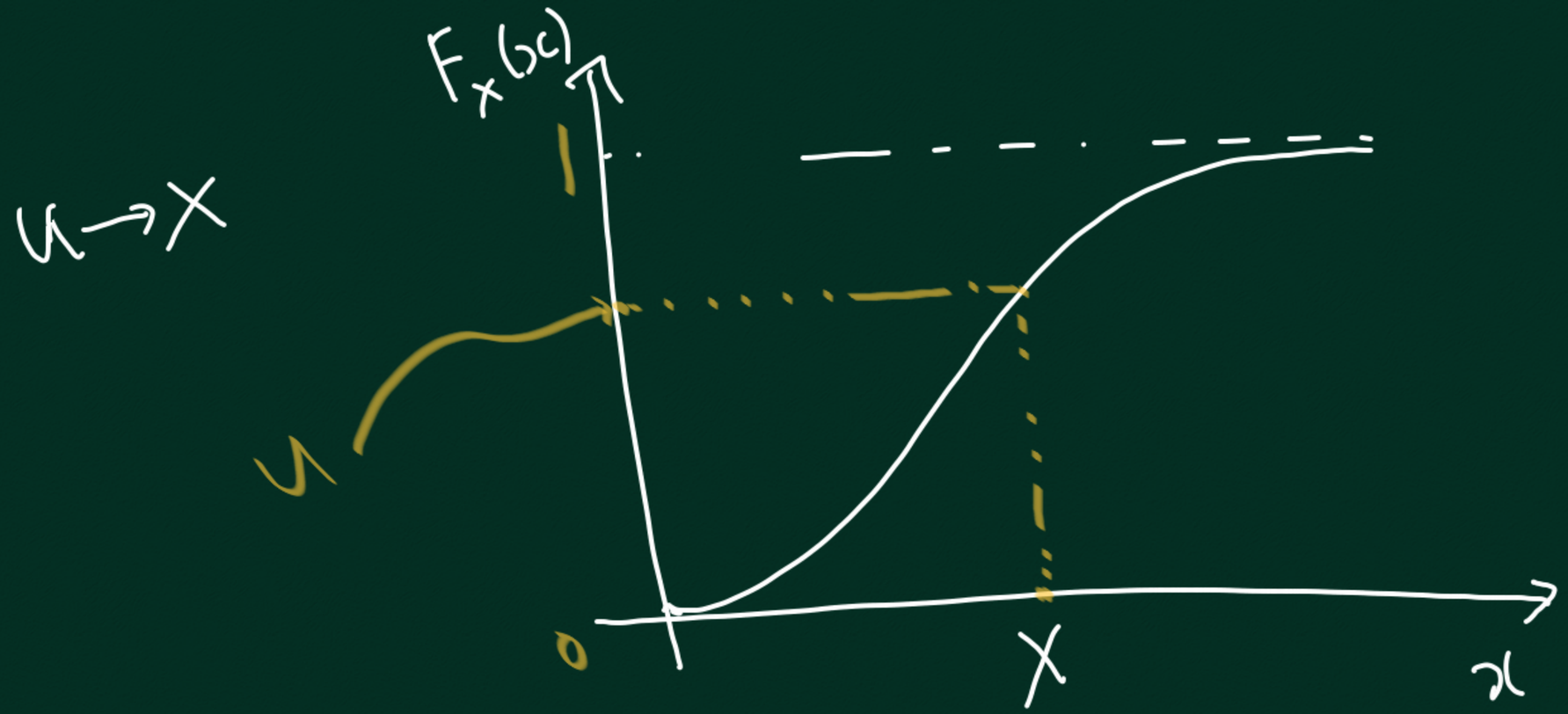
(pk, sk)

M selected

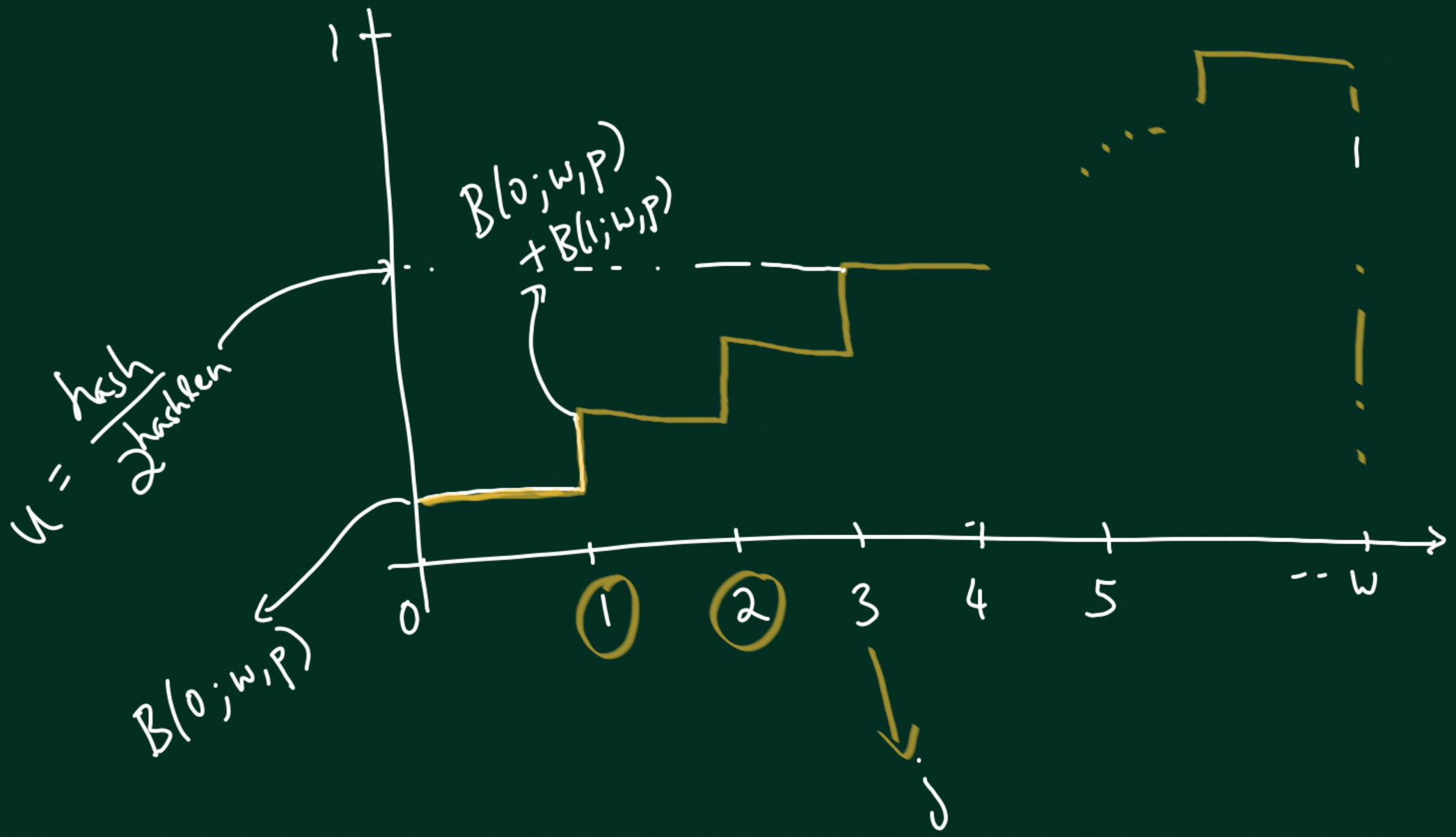
Distrib. of M? Binomial

$$B(k;\omega,p) = \text{Prob}(M=k) = \binom{\omega}{k} p^k (1-p)^{\omega-k}$$

Q. How to convert a unif r.v. $U \in [0,1]$ to any other r.v. X with c.d.f. $F_X(x)$



$X = F_X^{-1}(u)$


1
B(0;w,p)
+B(1;w,p)
u = hash / 2^hashlen
B(0;w,p)
0
1
2
3
4
5
... w
j

PHASE-0 (BLOCK PROPOSAL)

$$T_{PROPOSER} = 26$$

Suppose user has SORTITION output $\langle hash, \pi, j \rangle$

$$\text{priority of user} = \max_{i=1,2,\ldots,j} H(hash \,||\, i)$$

Ideally, user with highest priority is LEADER whose block must be chosen

priority

A → B_1 Blk with lowest hash

A → B_2

X (seen all) → B_1 → Phase1 → block/empty

C → B_3

Y ($B_2, B_3, \ldots$) → B_2

D → B_4

E → B_5

E → B_6

Z ($B_3, B_4 \ldots$) → B_3

committee

4ETBTPKJ