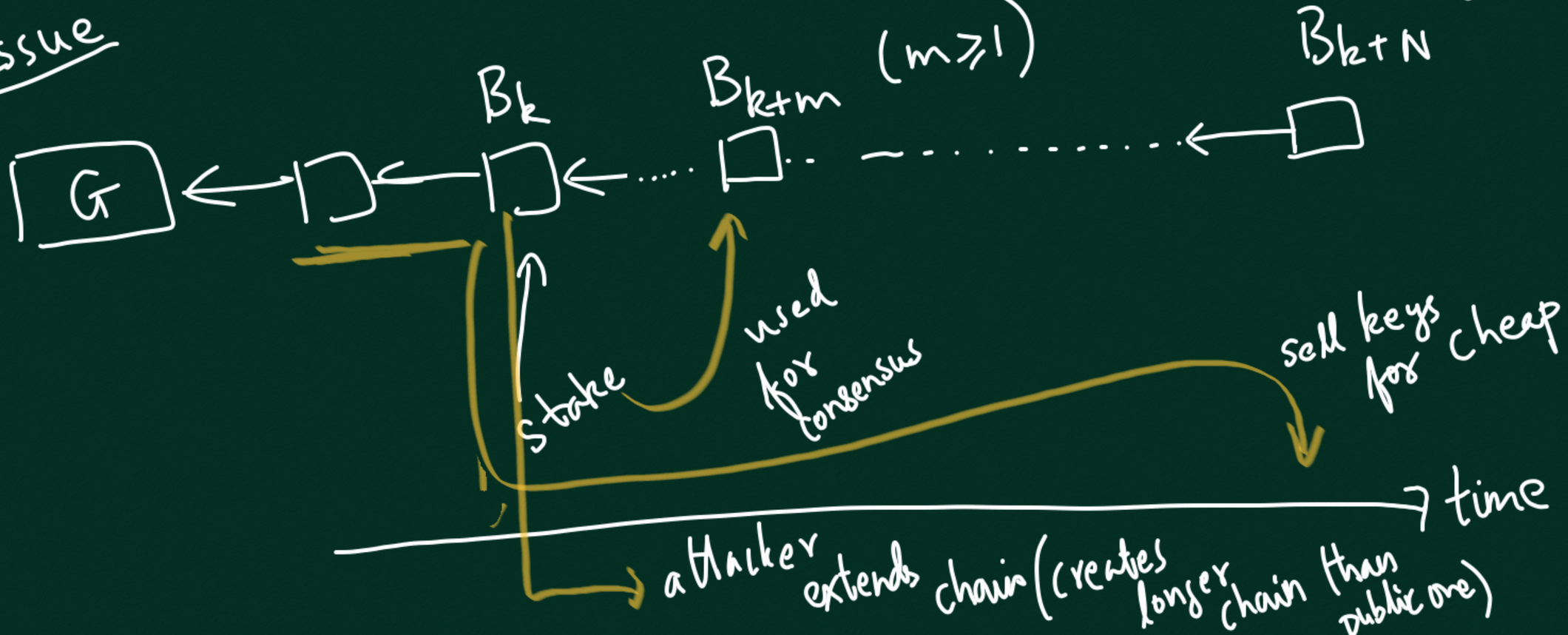
PoW vs. Naive PoS

Attendance

Energy

Noth. at Stake,
Long-range attacks
Pre-computing attack

Another Issue



PoW + PoS : last class

SLASHER: BUTERIN (2014)

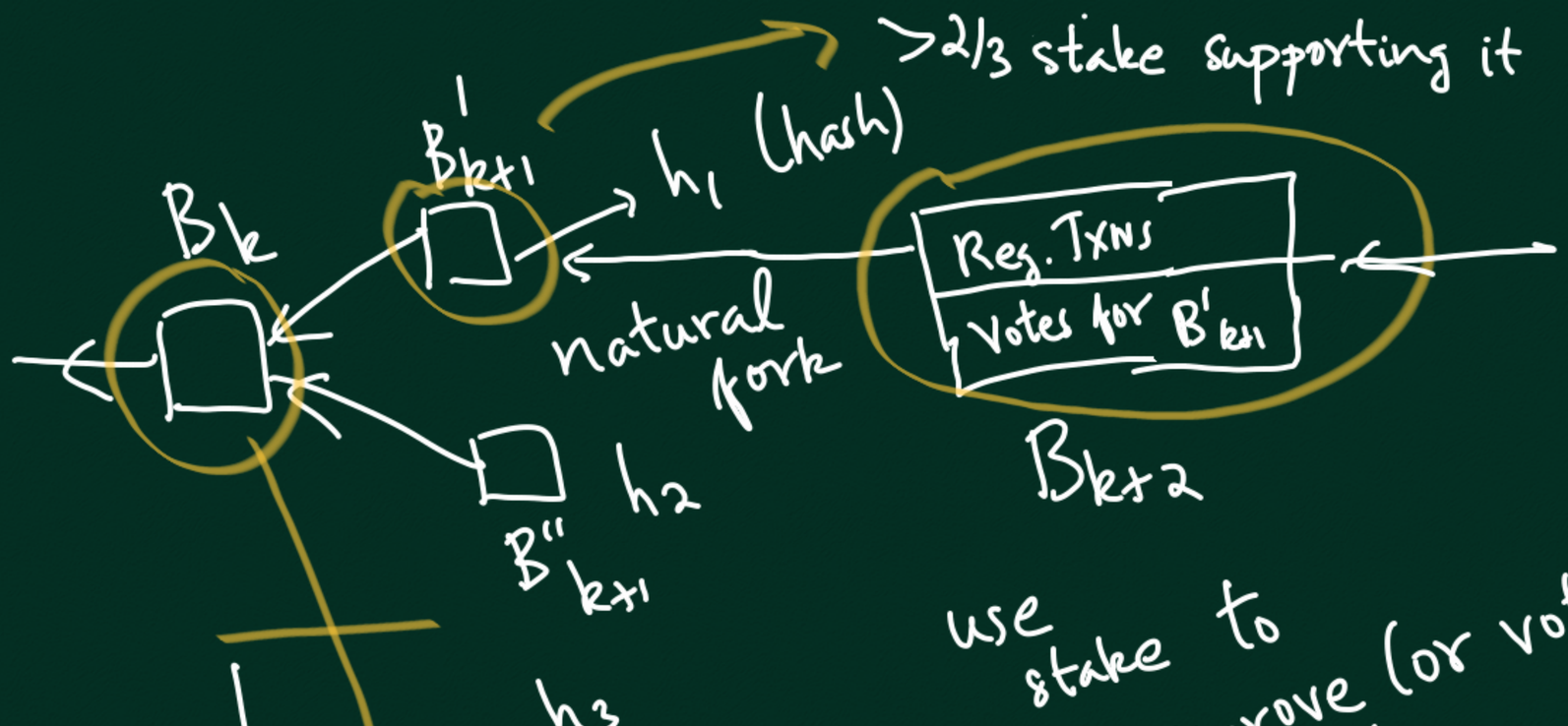
Energy

SLASHER

$\frac{1}{50}$ every year

BITCOIN

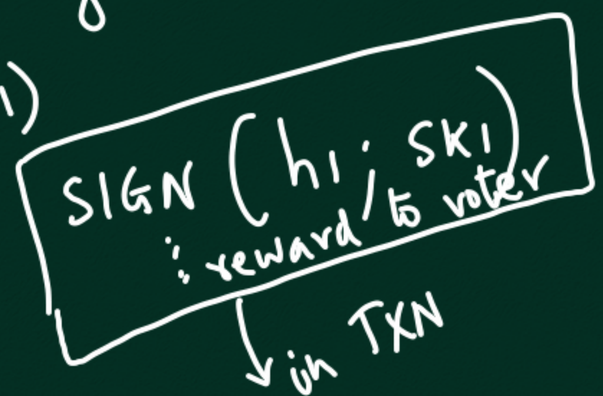
½ mining reward every 4 years



use stake to approve (or vote for) blocks

NOT to generate blocks

Naive:



Rules For Slasher

1. Blocks are mined by PoW, but mining reward decreases by factor of 50 every year

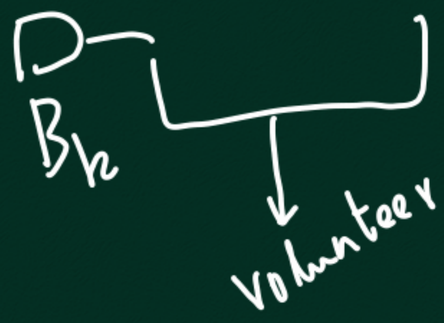
2. When B_k is produced, person with address 'a' checks if $\text{Hash}(a \,||\, \text{hash}(B_k)) < \text{bal}(a) * \text{target}$

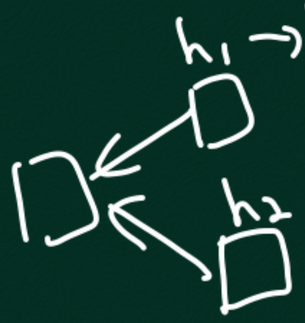
   - If true, then 'a' is potential signer of B_{k+3000}
   - $\text{hash}(B_k)$: possibly only hdr set so that true for 15 addresses on avg.
   - target: common

(3) Any potential Signer can <u>volunteer</u> to sign B_{k+3000}, by sending a volunteer txn on chain between B_{k+1} and B_{k+64}. It is called a

DESIGNATED SIGNER

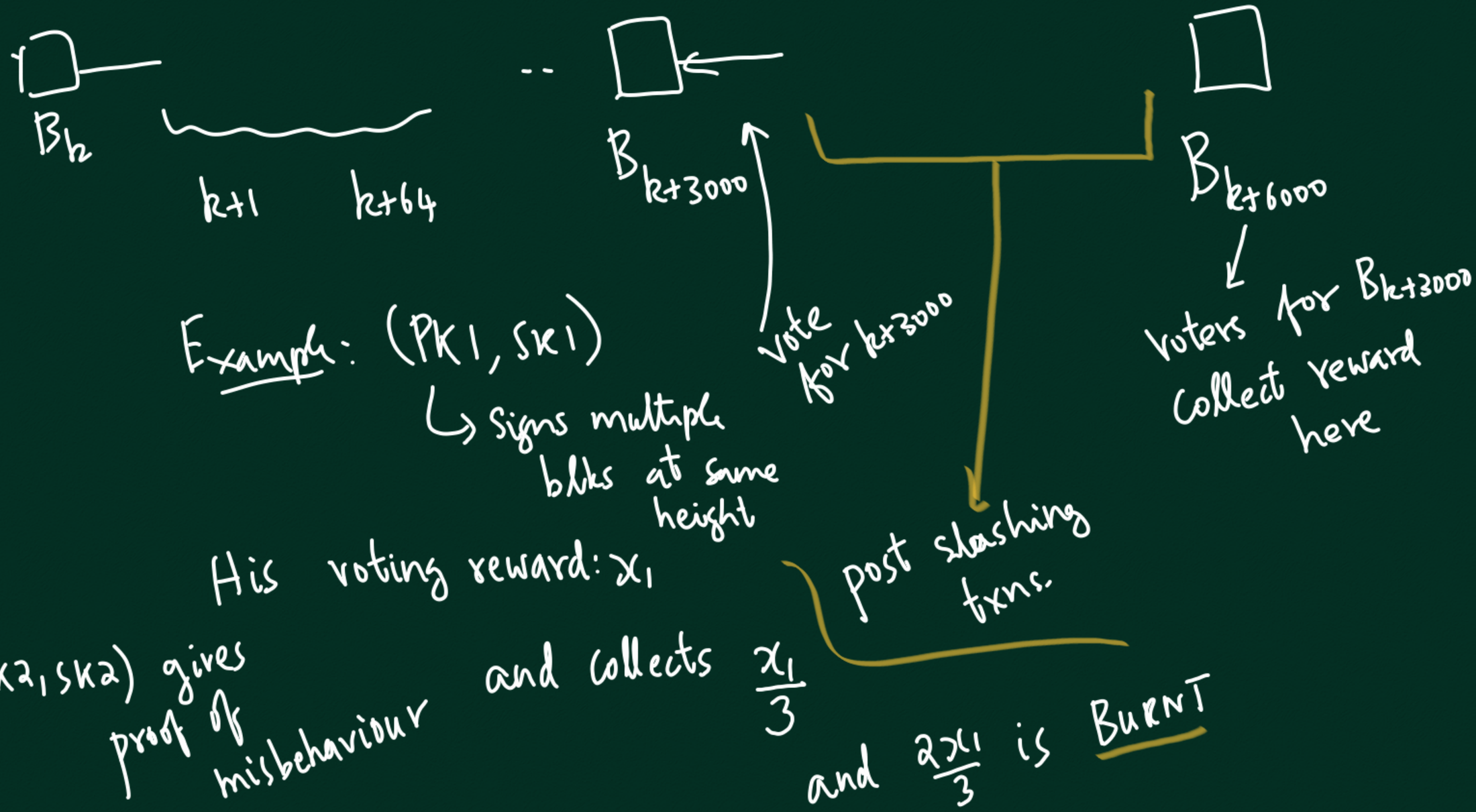
(4) When blocks at ht. k+3000 are generated, n votes for 1 blk at that ht





designated signer

SLASHING: Cut (slash) stake of misbehaving person



Example: (pk_1, sk_1)

↳ Signs multiple blks at same height

His voting reward: x_1

(pk_2, sk_2) gives proof of misbehaviour and collects $\frac{x_1}{3}$

and $\frac{2x_1}{3}$ is BURNT

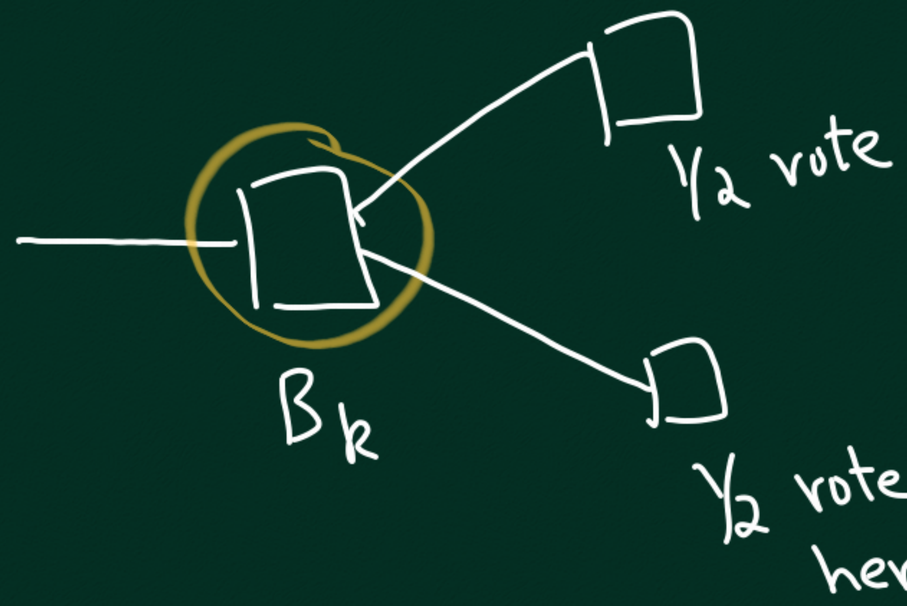
How To Burn? Pay to pub.key we know no one has secret key

Ex: PK = 0, pay to 0 address

---

5. Anyone can SLASH a misbehaving voter by publishing a txn before Blk_{+6000}.

6. Designated Signer collects voting reward after Blk_{+6000}



Q. What to do now?

Q. Why require $> \frac{2}{3}$ of ✓ Signers to vote for blk?

Committee

Suppose $< \frac{1}{3}N$ are malicious

Require $> \frac{2}{3}N$ to vote for blk for it to be valid

Prove: There cannot be 2 blks signed by $> \frac{2}{3}N$ of voters.

Suppose Set A signs h_1
B signs h_2 → Competing

$$N \geq |A \cup B| = |A| + |B| - |A \cap B|$$

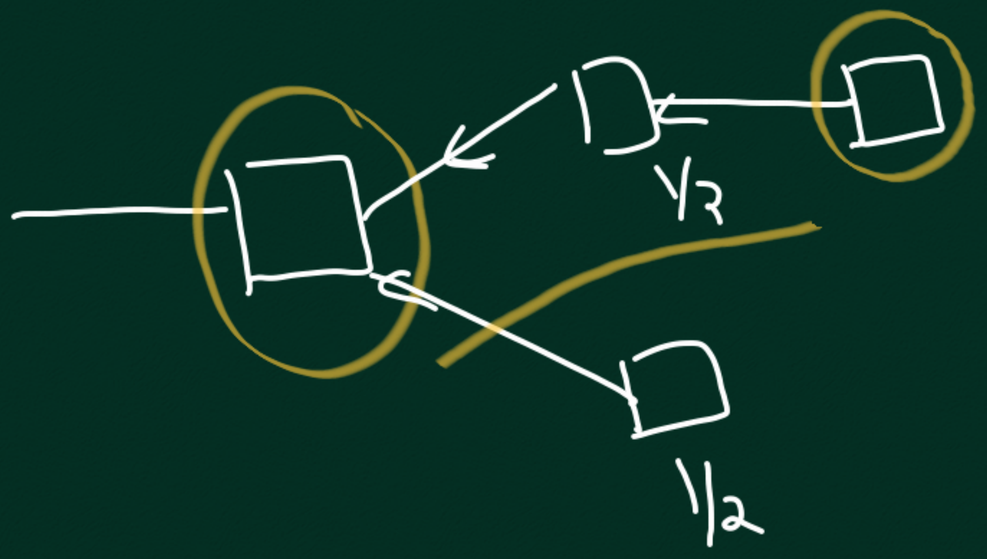
$|A \cap B|$ → must be malicious

size

$$|A \cap B| \geq |A| + |B| - N$$

$$> \frac{2}{3}N + \frac{2}{3}N - N = \frac{1}{3} \cdot N$$

$\Rightarrow$ # malicious nodes (voters) $> \frac{N}{3}$ → Contradiction

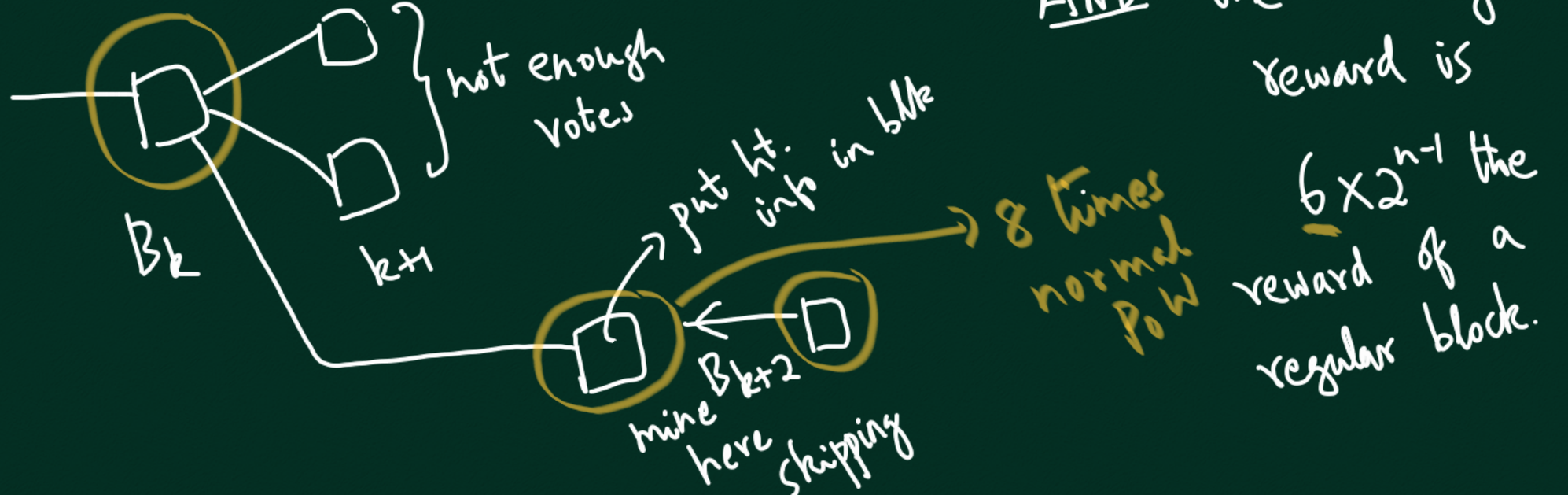


SLASHER

7.

Suppose a blk skips 'n' levels, then PoW reqd. to generate it is $8 \times 2^{n-1}$ a regular blk

AND the mining reward is $6 \times 2^{n-1}$ the reward of a regular block.

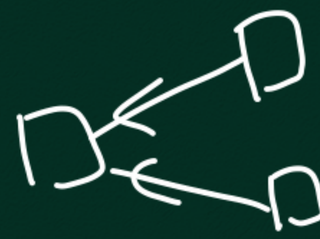


Problems addressed

Energy ✓

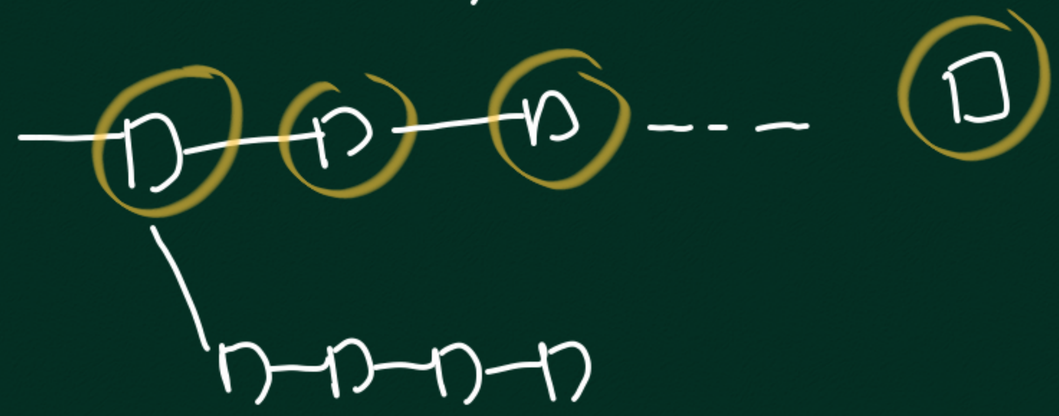
Nothing at stake?

→ SLASHED

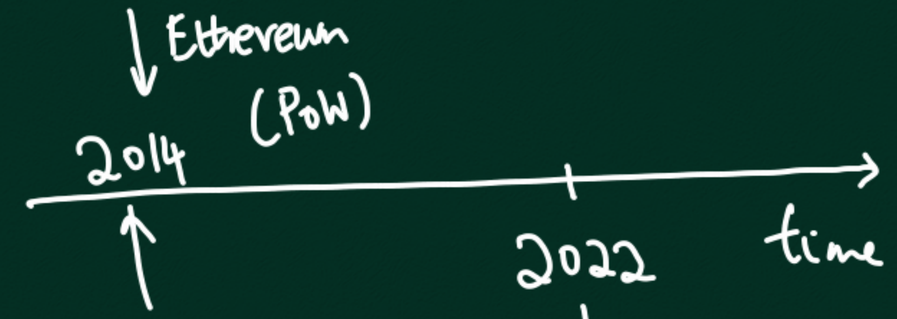


LONG-RANGE ATTACK → partly handled by PoW

→ requires purchase of old keys

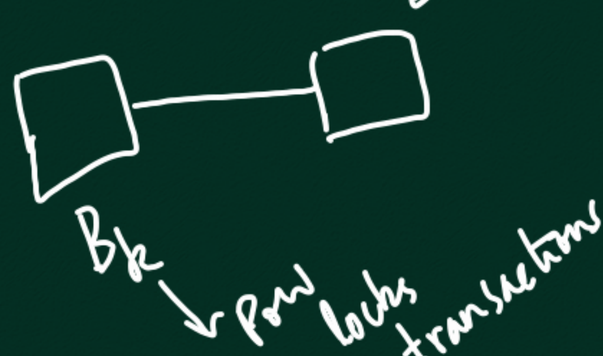


Pre-computing attack



Naive PoS

Slasher



RULES

(0) First 3000 blks mined only with PoW