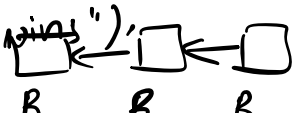
Nakamoto Consensus: ("longest chain wins"),

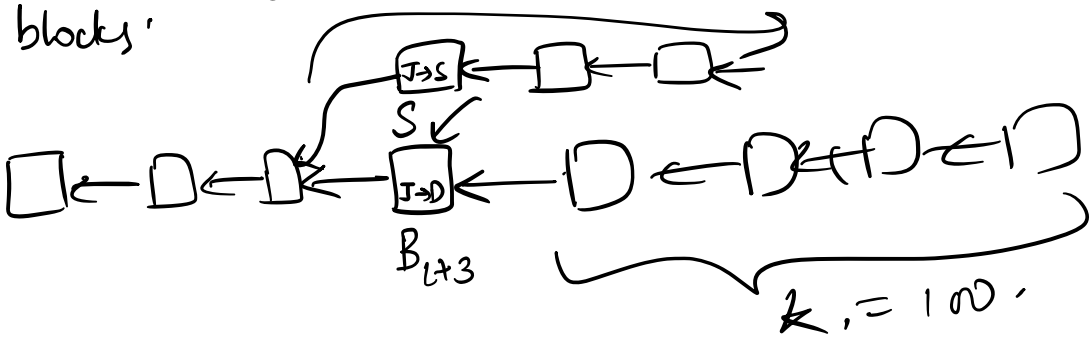


↳ Each party maintains a chain (tree).

↳ Each round, we will elect a "leader", unique & uniformly at random.

↳ leader creates a block B of txns & sends it to everyone. & add it to the longest chain.

↳ Each party will add B to their chain of blocks.



Scenario1: All parties are honest; rounds : 10 min.
msg sending < 10 sec.

Scenario 2: 30% (49%) of the parties are ; "
Byzantine (corrupt)

honest 70%.
malicious 30%.

> 0.5.

P_R (honest is elected in a round) $= 0.7$

When a block is at (depth k.)

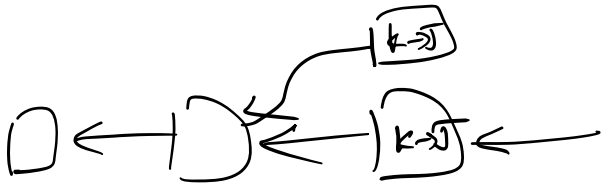
Pr(private chain attack) $\leq \exp(-k)$.

2^{-128}

depth 6.

Scenario 3: Byzantine faction 80%.

→ longest chain will be a malicious one.
→ malicious parties will make honest parties agree on ~~different things~~ conflicting txns.



→ Notion of rounds & selection of unique & random leader.
→ Fixed of parties.

$H(x) = y$.

Collision resistance: It is infeasible to find x & x' s.t. $H(x) = H(x')$ when $x \neq x'$.

Pre-image resistance: Given y, it is hard to find x.

Puzzle:

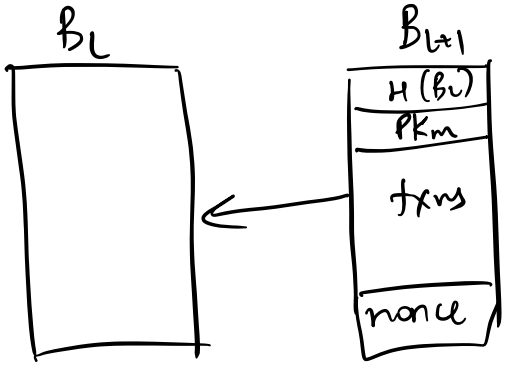
$H(x) = \underbrace{0000000}_{k}$, anything.

x: PK, hash txns, nonce

2^k

$(1/2)^k$

0 ↑ 1/2.



$H(H(B_L) \| PK_m \| txns \| nonce) =$

"permissionless":

2009: CPUs.

~~GPU~~: GPUs

2012-2015.

ASIC