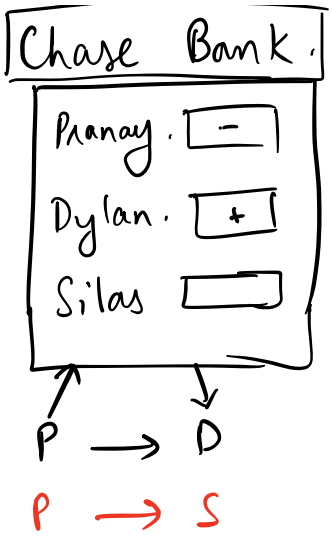
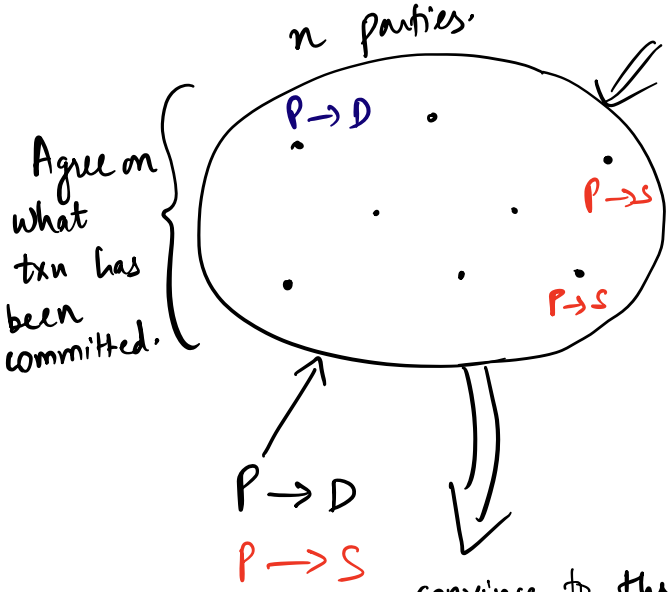




listen to $\frac{n}{2}+1$ parties saying "P → D".

t corrupted parties

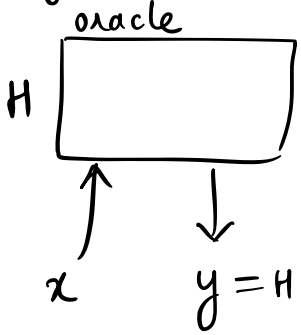
↳ listen to $\geq t+1$ parties saying "P → D".

1980: Byzantine Generals Problem.

2008: Bitcoin, by Satoshi Nakamoto.

Nakamoto consensus: "longest chain wins".

Cryptographic hash function:



If x was queried, return H(x)=y.

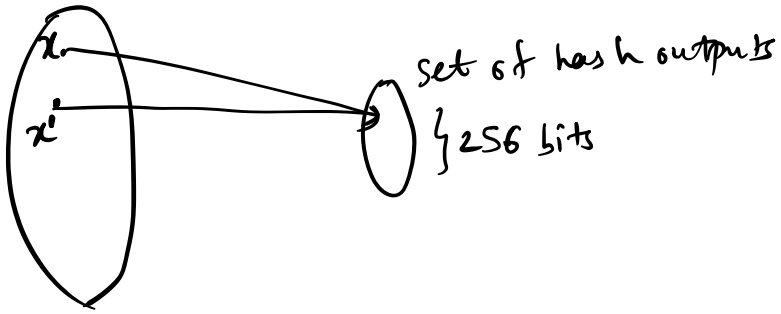
Toss random coins (256 coins)

↓ output y.

Remember (H(x)=y).

↳ deterministic.

↳ x: arbitrarily large input
y: fixed size (256 bits / 512 bits).



$\exists\ x, x'$ s.t. $H(x) = H(x')$.

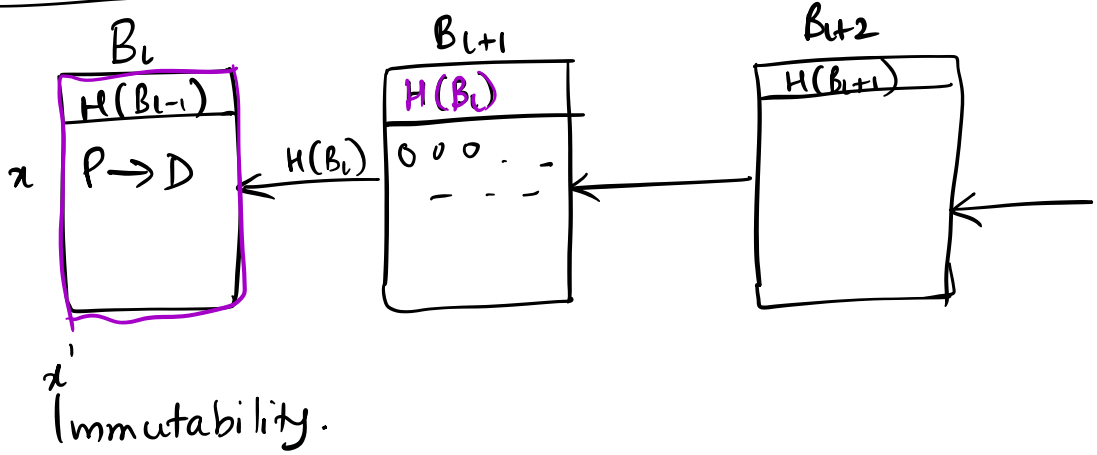
Collision resistance:
It is infeasible to find x & x' s.t. $H(x) = H(x')$

⇓

Second pre-image resistance: Given x, it is infeasible to find x', ...

⇓

Pre-image resistance: Given $H(x)$ it is hard to find x.



Immutability.

longest chain wins rule:

→ Each party maintains many different chains $\mathcal{C}$

→ Protocol proceeds in rounds:

↳ In each round, we elect a unique random leader L.

↳ If L has atleast one chain in its storage, it picks the longest chain $C \in \mathcal{C}$, creates a new empty B and attaches $C \leftarrow B$.

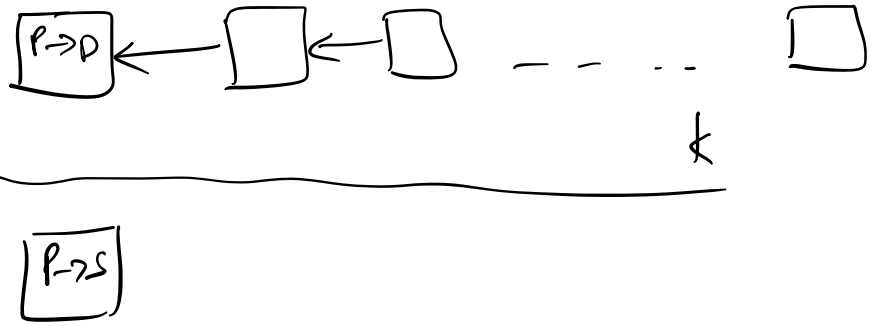
o.w. if $\mathcal{C}$ is empty, start a new chain with a block containing $P \to D$ or. $P \to S$.

→ Announce chain to all other parties.

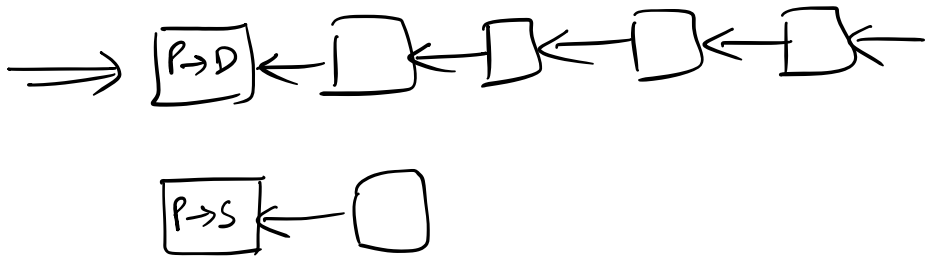
(If some party receives any information, send it to everyone)

Commit: when the longest chain is k blocks deep; commit the first block.

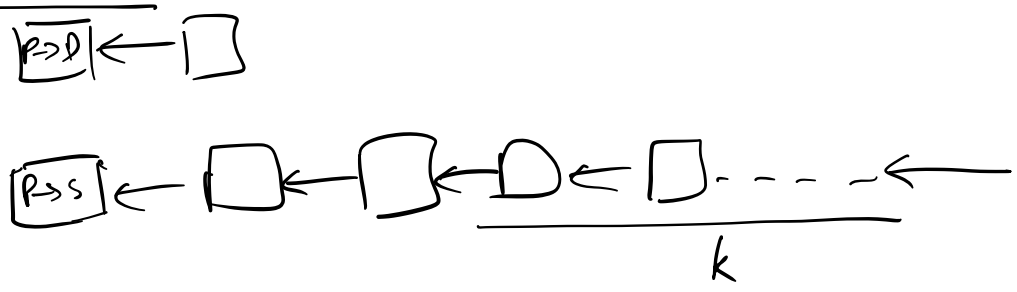
Scenario 1: All parties are honest.



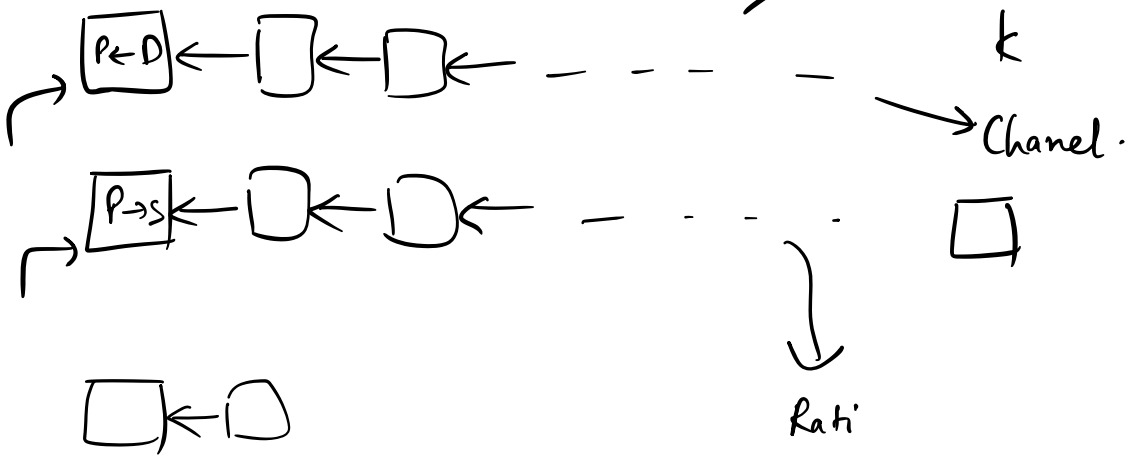
Scenario 2: Some malicious pairs (50%.)



Alternative exec:



Scenario 3: # malicious parties ≥ 90%
"Private" ≥ 50%



Scenario 4: # malicious parties = 49%

honest > # malicious.

P. (honest is elected in a round) > 1/n

Pr [honest is elected ...] > 1/2

when some chain is length k,

Pr[Private chain attack succeeds] $\leq \exp(-k)$.

e^{-128}

30% > 0.2