→ Efficiency: latency, throughput, communication complexity.
7 tx/sec.

space/storage.

Energy —

→ Adversaries: $n$ parties, $t$ are corrupt ↳ Crash/Omission (Paxos) semi-honest
↳ Byzantine/Malicious.

honest/Byzantine. $t < \frac{n}{2}$, $t < n/3$.

$f$

→ Accountability: detecting fault.

→ Rational & only some of them Byzantine.

↳ MEV (Miner extractable value).

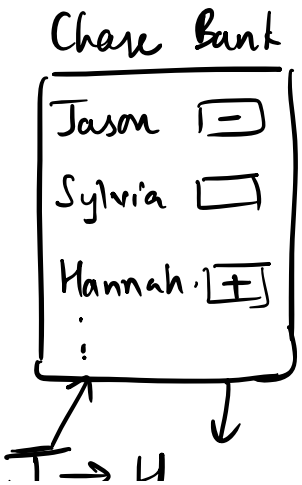
↳ Fairness.

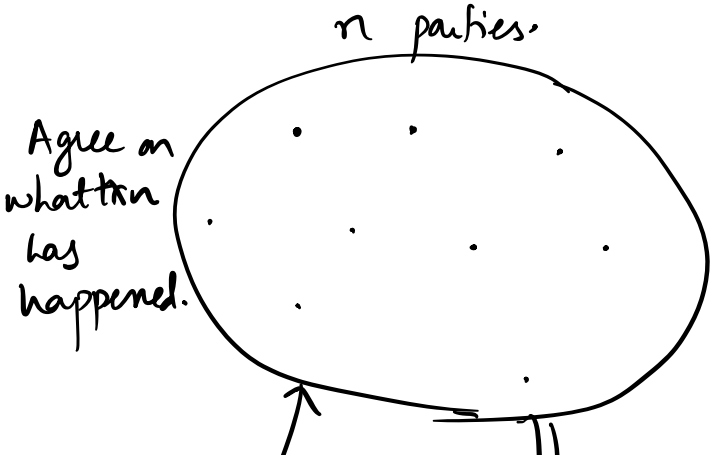
→ Privacy.

---

Bitcoin / Nakamoto Consensus (2008 - Satoshi Nakamoto)

Byzantine Generals Problem (1980)
Lamport Shostak Pease.



$J \to H$.

$J \to S$.

convince to the world that "tx" happened.

---

- All of you share $J \to S$

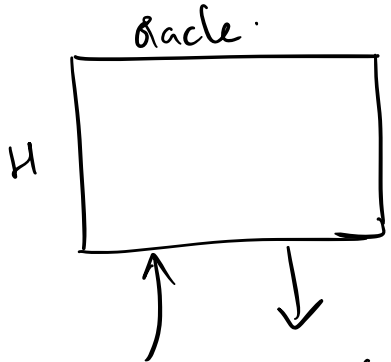
- if $t+1$ parties say $J \to S$.

  ⇓

  majority $t < n/2$.

---

Cryptographic Hash functions




If $x$ was queries, return $H(x)=y$.

Toss random coins (256 coins)

↓

output $y$.

Remember $H(x) = y$.

$x$.

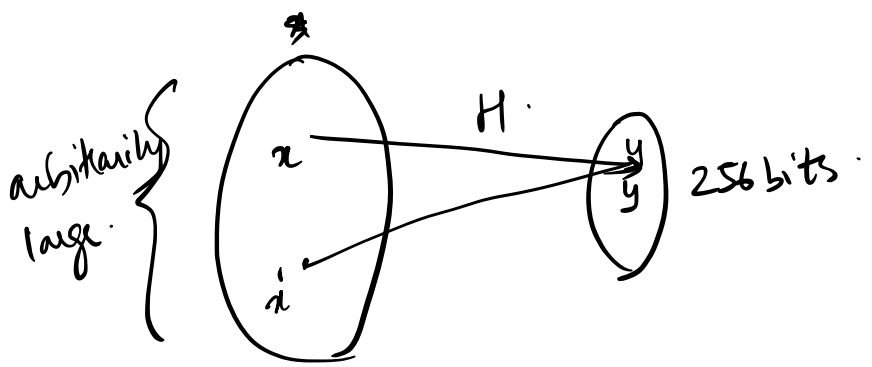
(any length)

$y = H(x)$.

↓

(fixed length)

256 bits.



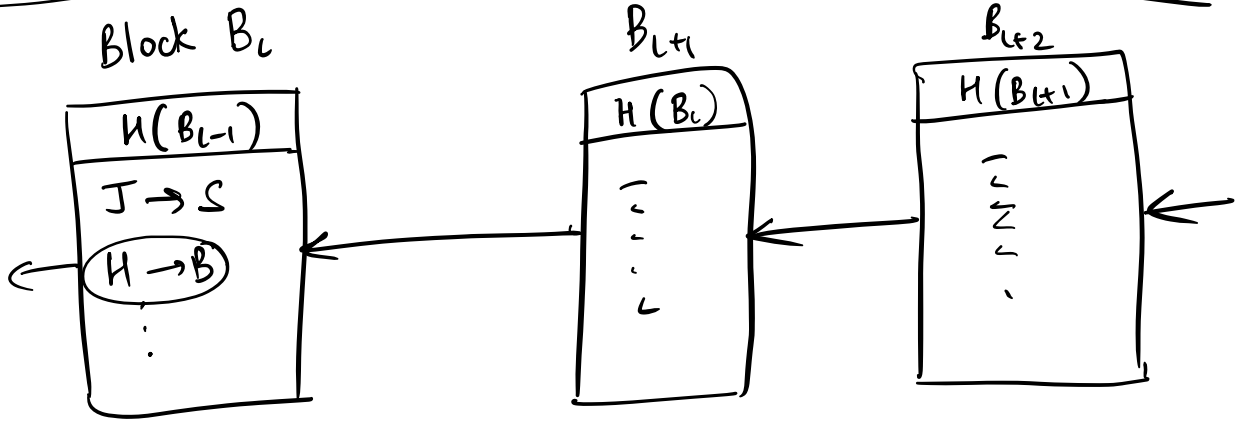
Collision Resistance: It is infeasible to come up with

$x$ & $x'$, $x \neq x'$, $H(x) = H(x')$.

SHA512, SHA 256...

↳ SHA1 ✗

MD5




Immutability: $H(B_L)$