→ Efficiency: latency, throughput, communication complexity.
   \[ t + 1 \text{sec.} \]
   space/storage.
   Energy \[ \text{(Paxos semi-honest)} \]
   crash/ omission
   → Adversaries: \( n \) parties, \( t \) are corrupt \( \subseteq \) Byzantine/Malicious.
   honest/Byzantine, \( t < \frac{n}{2} \)
   \[ t < \frac{n}{3} \]
   → 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.
- All of you share $J \rightarrow S$.
- If $t+1$ parties say $\# J \rightarrow S$.
  \[ \text{majority } t < n/2, \]

\underline{Cryptographic Hash Functions}

\[ H \]

\begin{align*}
\text{If } x \text{ was queried, return } H(x) = y. \\
\text{Toss random coins (256 coins)} \\
\text{output } y. \\
\text{Remember } H(x) = y.
\end{align*}

\[ x \overset{\text{(any length)}}{\longrightarrow} y = H(x). \]

\[
\text{(fixed length)} \quad 256 \text{ bits.}
\]
Collision Resistance: It is infeasible to come up with \( x \& x' \), \( x \neq x' \), \( H(x) = H(x') \).

SHA-512, SHA-256...

MDS

Block \( B_c \)

\( H(B_{c-1}) \)

\( J \rightarrow S \)

\( H \rightarrow B \)

\( B_{c+1} \)

\( H(B_c) \)

\( B_{c+2} \)

\( H(B_{c+1}) \)

Immutability: \( H(B_c) \)