\( n, t \) are malicious, committing a single \( \text{txn} \).

\( \rightarrow \) Committing a single \( \rightarrow \) many

\( \rightarrow \) Notion of rounds; message delays

\( \rightarrow \) fixed set of parties.

---

Committing a single \( \text{txn} \) to many \( \text{txns} \):

Large blocks:

\( \rightarrow \) we may not know of all \( \text{txns} \)

\( \rightarrow \) they take a lot of time to propagate.

---

Run consensus protocol multiple times:

\[ \begin{array}{ccc}
\text{Instance 1} & : & \text{Instance 2} & : & \text{Instance 3} : \\
\text{Proposed} & \{\text{txn}\} & \{\} & \{\text{txn}\} & \{\} \\
\text{Votes} & \uparrow & \uparrow & \uparrow & \uparrow \\
\text{txn}_1 & \uparrow & \uparrow & \uparrow & \uparrow \\
\end{array} \]

\[ \rightarrow \] Each block contain some \( \text{txns} \): \( 1\text{MB}(\text{max}) \)

\[ \rightarrow \frac{L_3}{4\text{MB}}. \]
n parties, t malicious:

X fixed set of parties, I do not know each other

Join or leave the system at any time.

"Permissionless": no identities associated with them.
Assumption: The resource held by any adversary is less than that held by honest parties.

\[ H(\text{random}) \rightarrow y \quad (\text{infeasible}) \]

\( \text{Bt+1} \quad 0 x x x \cdots \)

\( \text{probabilistic} \)

\[ H(\text{txs|nonce| } r) \rightarrow 0000 \quad \rightarrow \]

\[ H(Bi) \]

\[ H(Bi) \quad \text{txs} \]

"pseudonyms".
\[ H(\text{block} | \text{nonce} | H(B_i)) \Rightarrow 000000 \ldots \lambda \]

keep changing.

\[ \text{common} \]

k block

\[ 2^{-x} \]

easy moderately hard-trying.

collision.

How many zeros?
SHA-256: collision?

After how many blocks, can I think of SHA256 as being insecure?