1. Raft clusters need to be small. Leader election does not scale.
   Split votes.

2. Raft is designed for data centers.
   \[ Bcast\ time \ll\ Election\ timeout \ll\ MTBF \]
   \[ \Rightarrow \] partitions are rare.

3. Raft is designed for mostly static membership.
Bitcoin - Decentralized Bank
- Peer-to-peer system
- Open membership
- Wide area
- Frequent failures
- Many (1000s) of nodes

Proof of Work
\[ H(\text{input}) \rightarrow 256 \text{ bit output} \]

\[ \log_{137} y \text{ hard} \]

\[ y = H(x) \uparrow \]

\[ \geq 256 \]

Find \( x \) such that \( H(x) \)

starts with 0's

any \( x \) wins \( \frac{1}{k} \) prob \( 2^{-k} \)

verify \( x \) in \( O(1) \) time
Block 1

\[ H(\text{Block1}) = 0 \]

Block 2

\[ H(H(\text{Block1})) = 0 \]

\[ H(11 + x^2) \quad 11x = 0 \]
Splits of length $l$ are exponentially unlikely.

- Broadcast blocks when solved
- $T(\text{Broadcast}) < T(\text{Solve puzzle})$

Tuning parameter $(k)$
Commit threshold + confirm