Proof of Work System

- A system that requires miners to do computational work to add blocks.
- Any peer can replace the blockchain.
- The proof-of-work makes it expensive to generate corrupt chains.
- Manageable to submit one block, unproductive to generate an entire chain.

Proof of Work System

- Hashcash was a proof-of-work system to prevent email spamming.

Difficulty = 6

Hash = 000000haxi2910jasdflk

- Generate hashes until a one with the matching leading 0's is found.
- A "nonce" value adjusts in order to generate new hashes.
- This computational work is "mining."

Proof of Work System

- The difficulty sets a rate of mining.
- Bitcoin sets the rate to a new block around every 10 minutes.

51% Attack

- A dishonest miner has more than at least 51% of the network's power.
- A 51% attack for bitcoin would be more than $6 billion (start of 2018).

Dynamic Block Difficulty