Scale-related security issues

Peter Todd

Sept 12th 2015

What are we trying to accomplish?

Bitcoin is a

~~payment system~~

~~micropayment system~~

~~settlement system~~

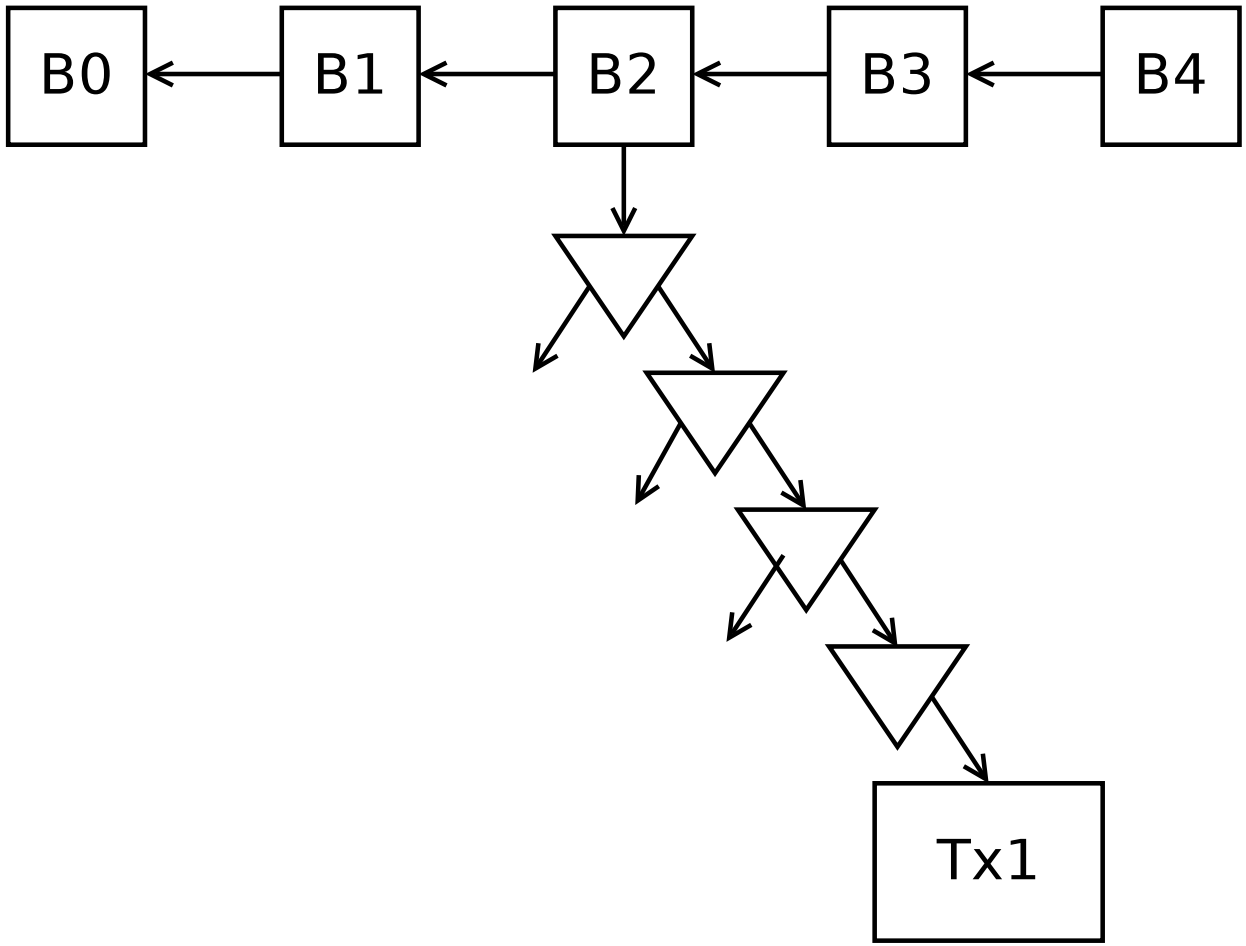
~~store of value~~

~~smart contract platform~~

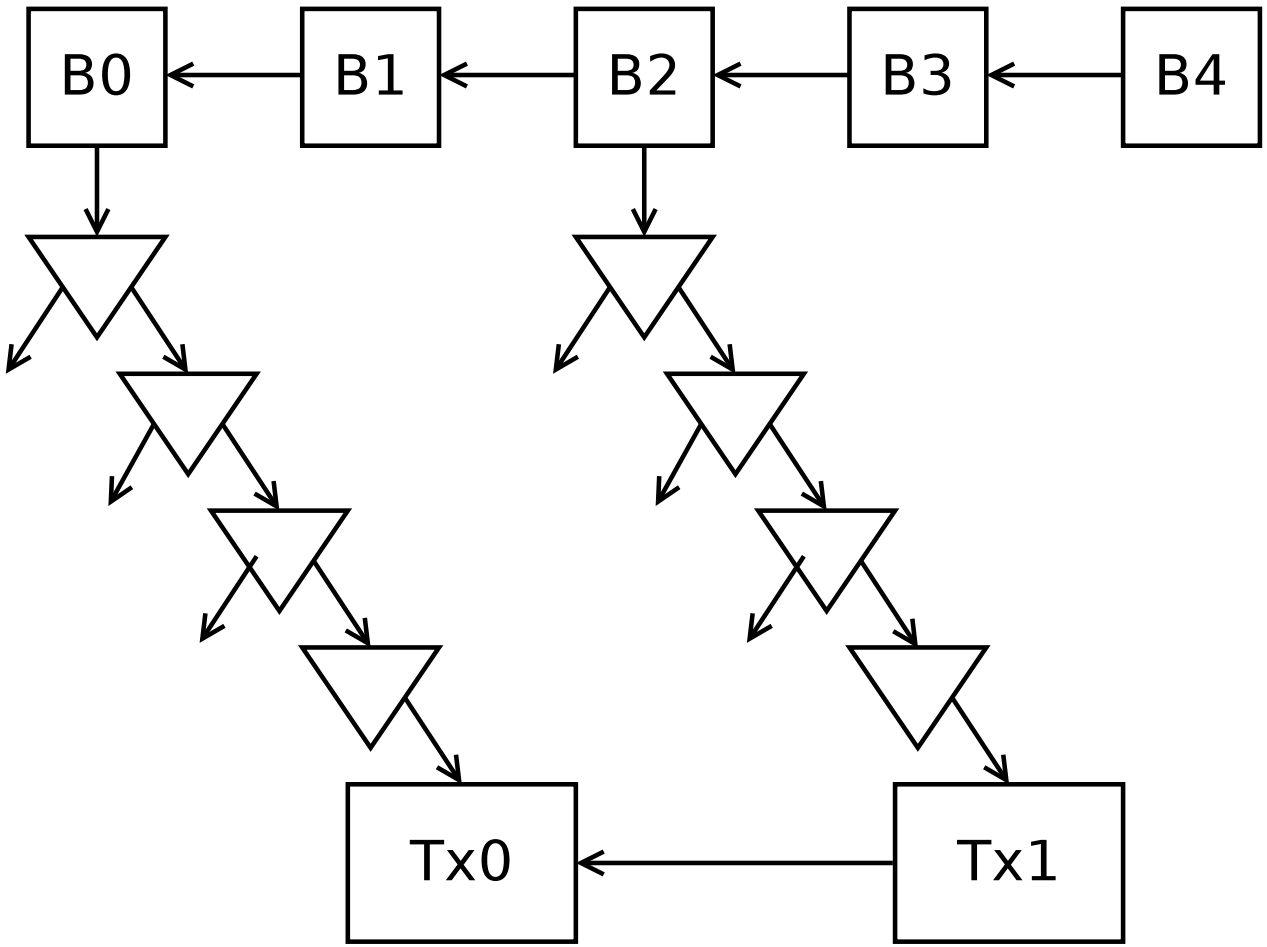
~~ponzi scheme~~

Rorschach test

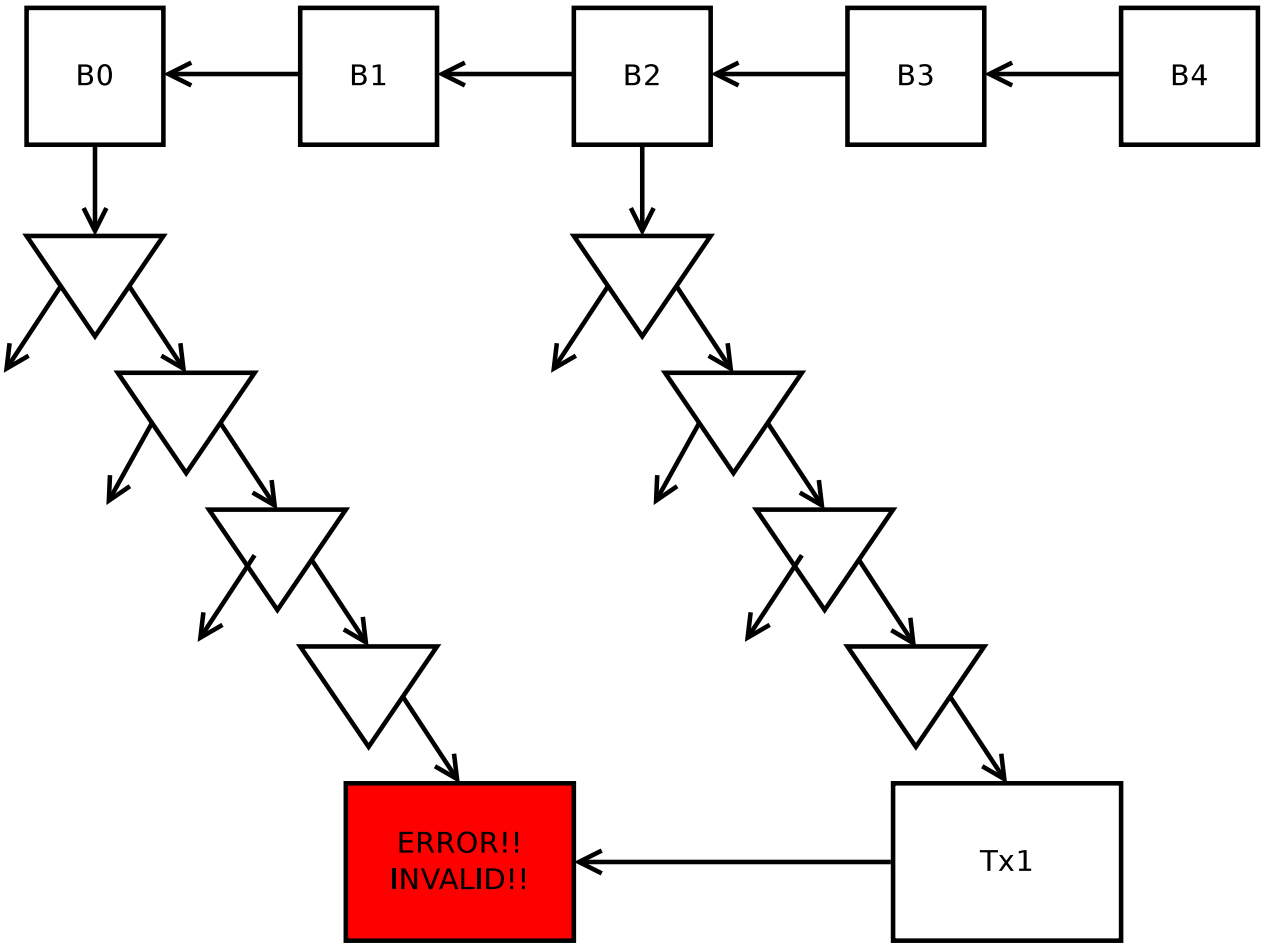
What are we trying to prevent?



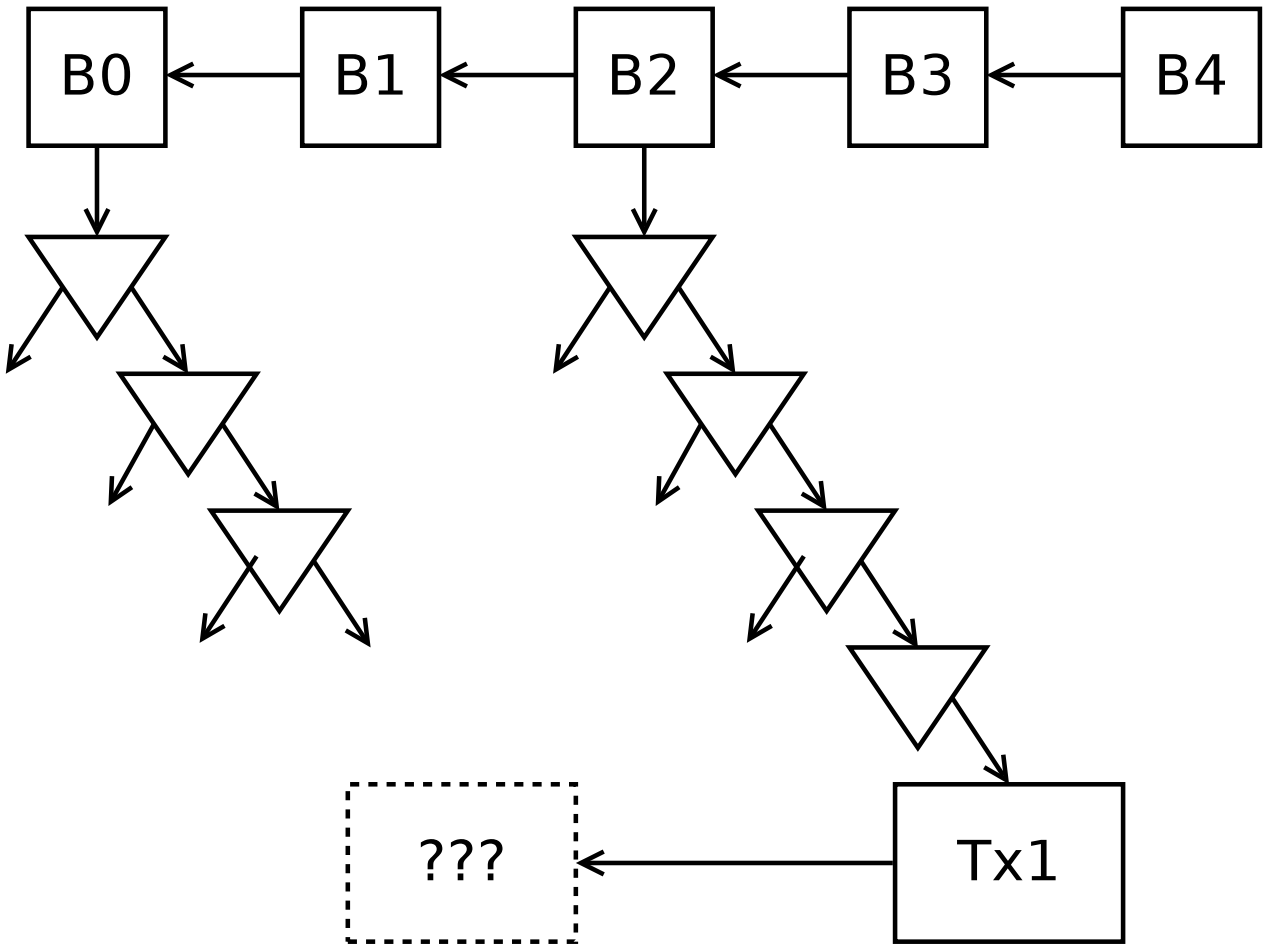
Valid history



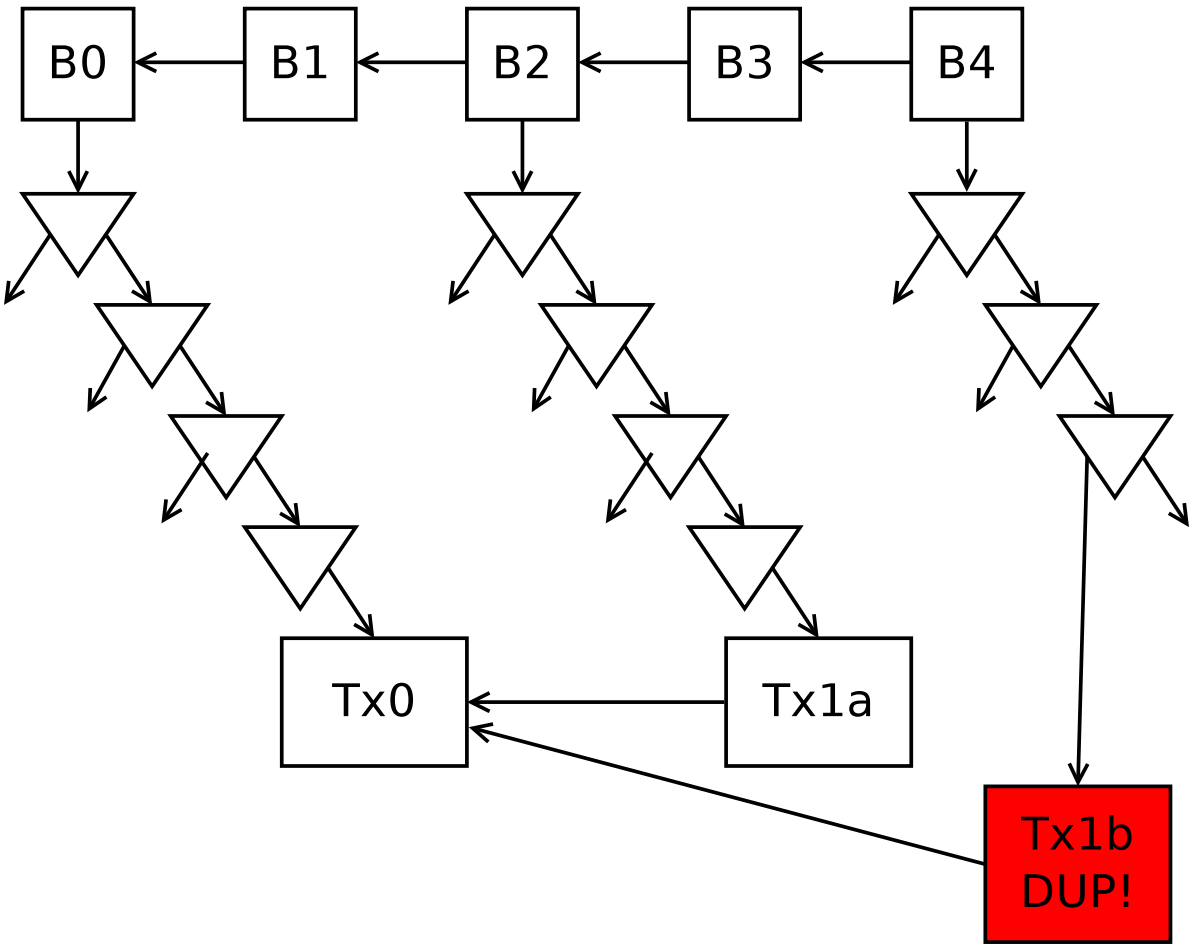
Invalid transaction



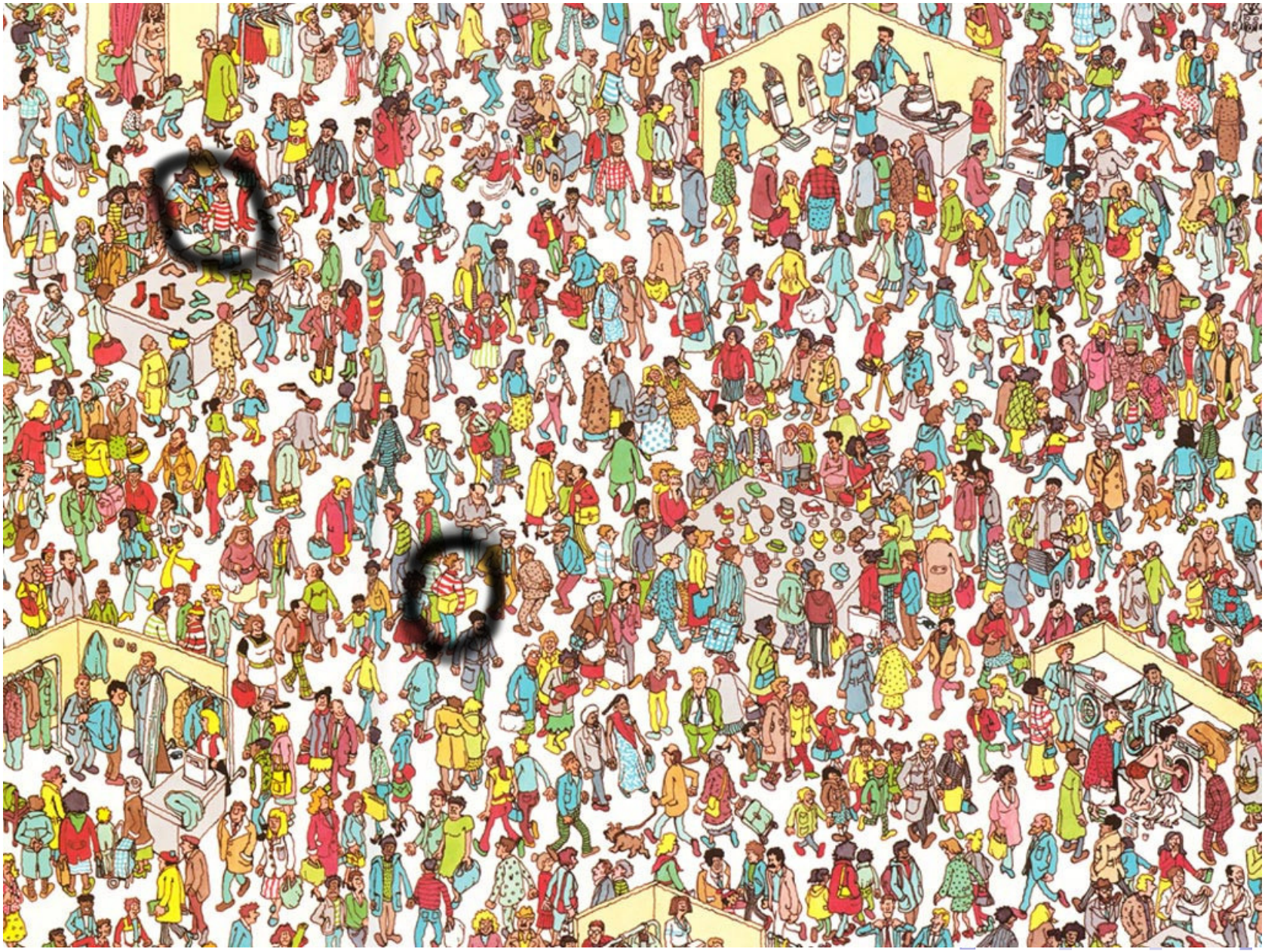
Missing input



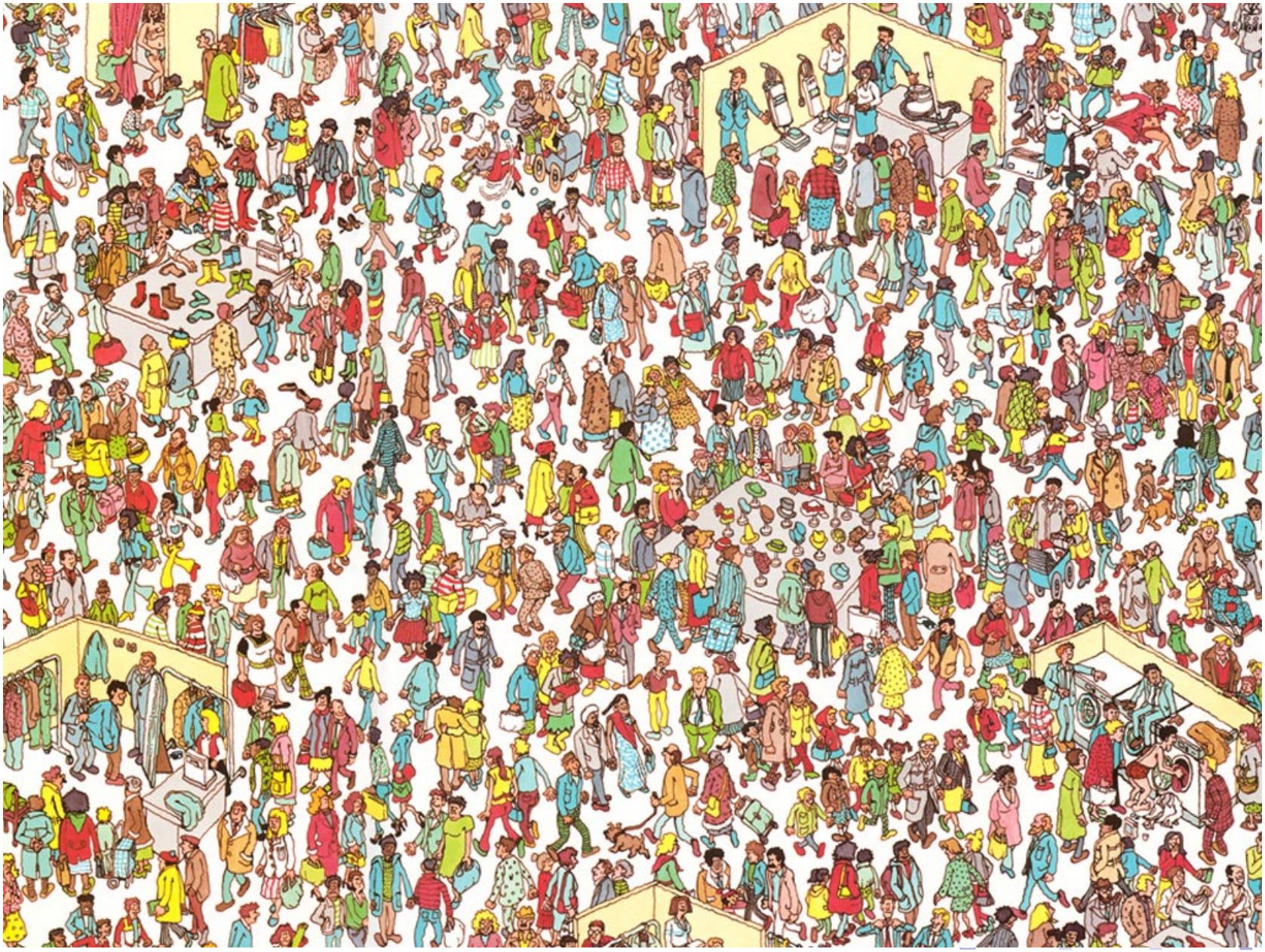
Doublespend



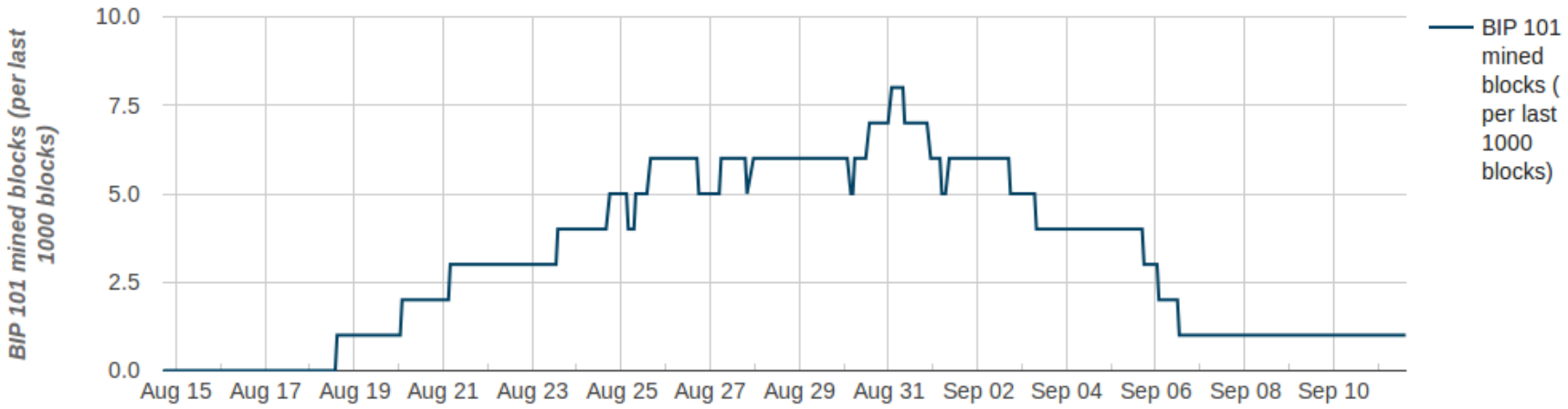
Doublespend Fraud Proof



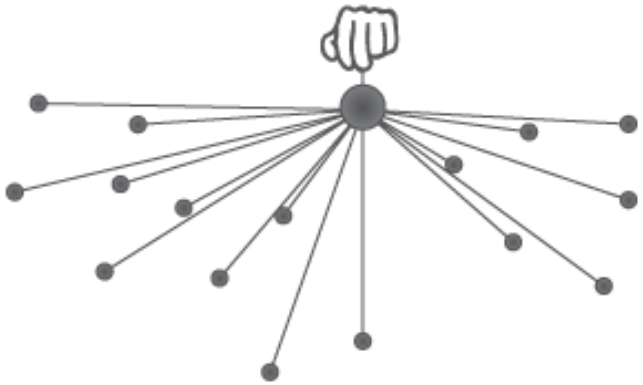
Doublespend - Miner perspective



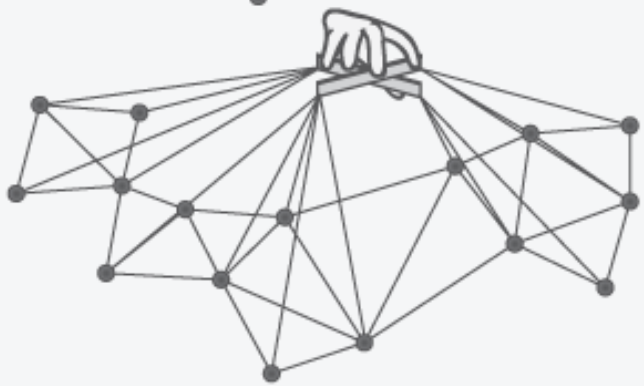
Reliability - External attack



Centralization - Single Points of Failure

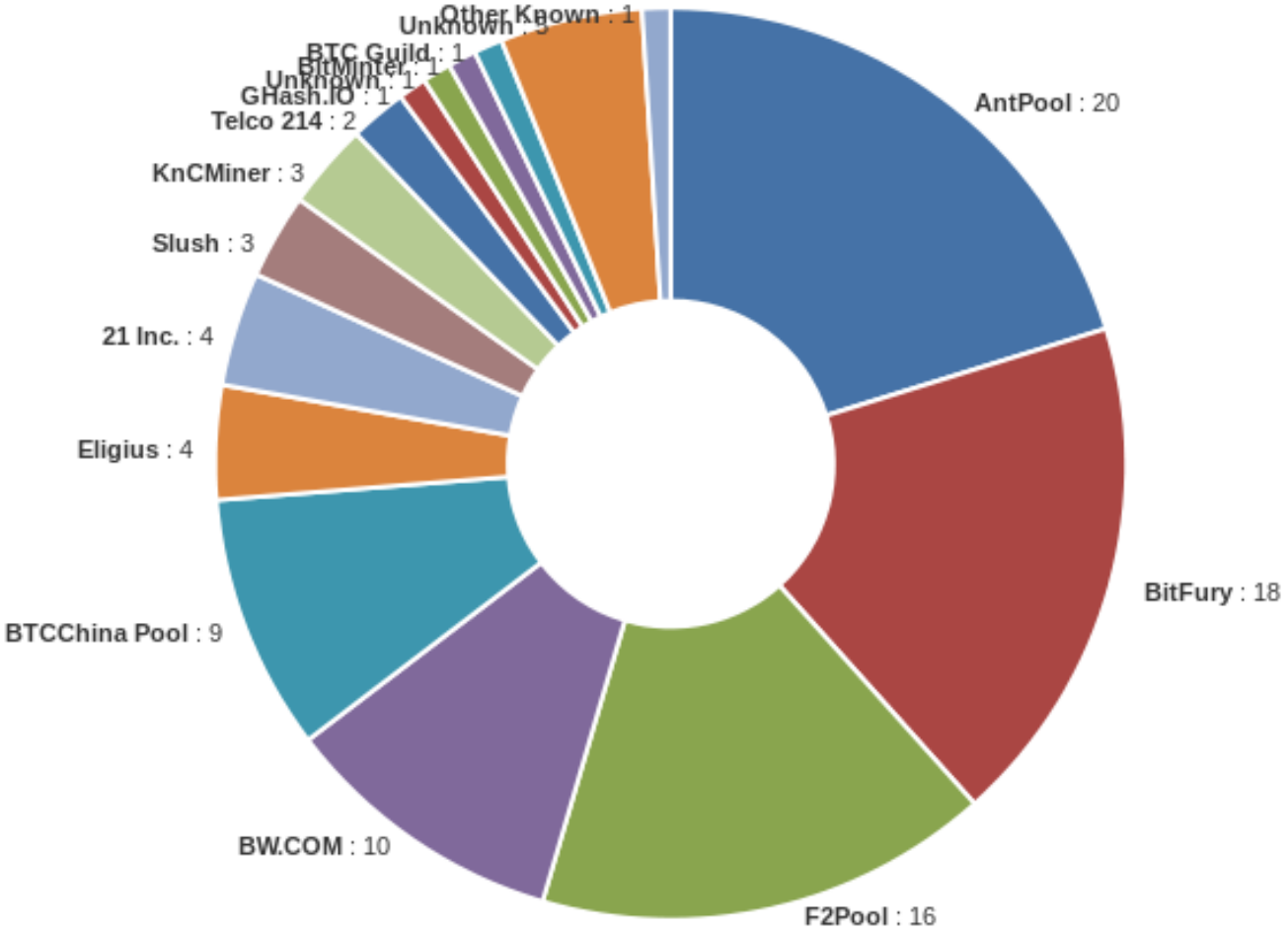


Centralized



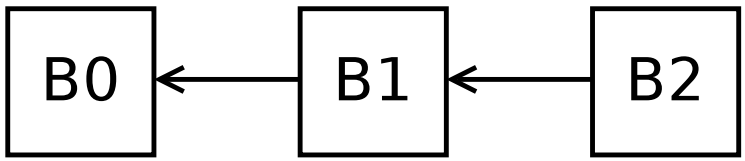
Distributed

Miner centralization

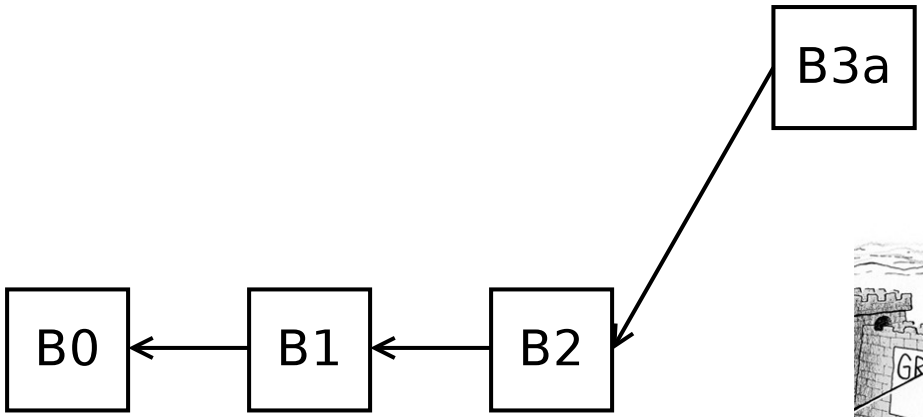


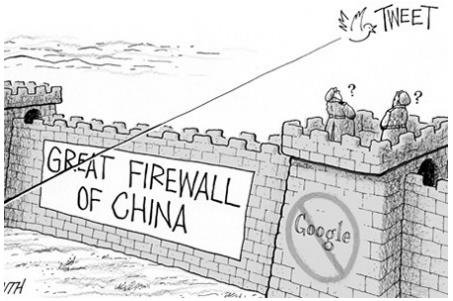
Miner centralization

Large miner advantage

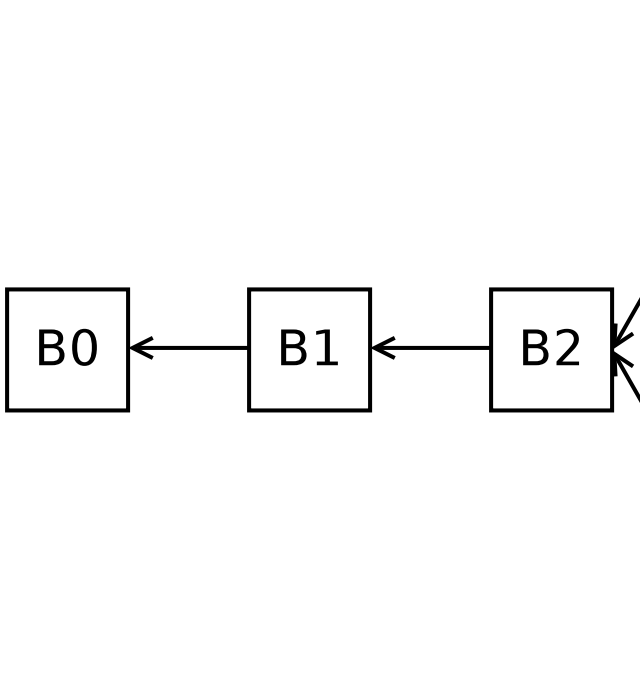


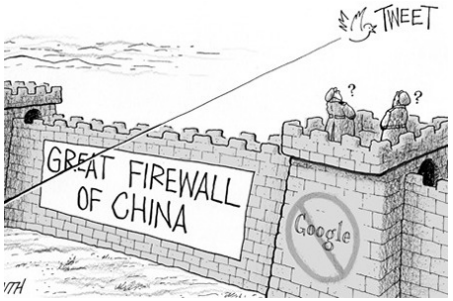
Large miner advantage



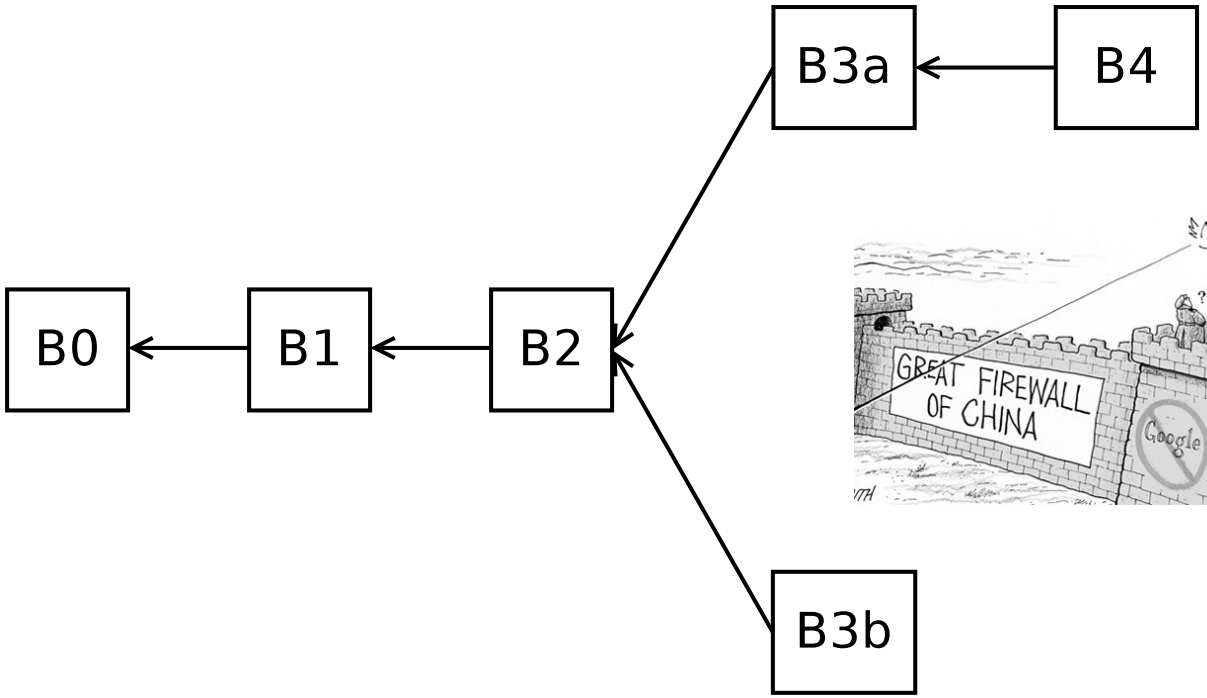


Large miner advantage

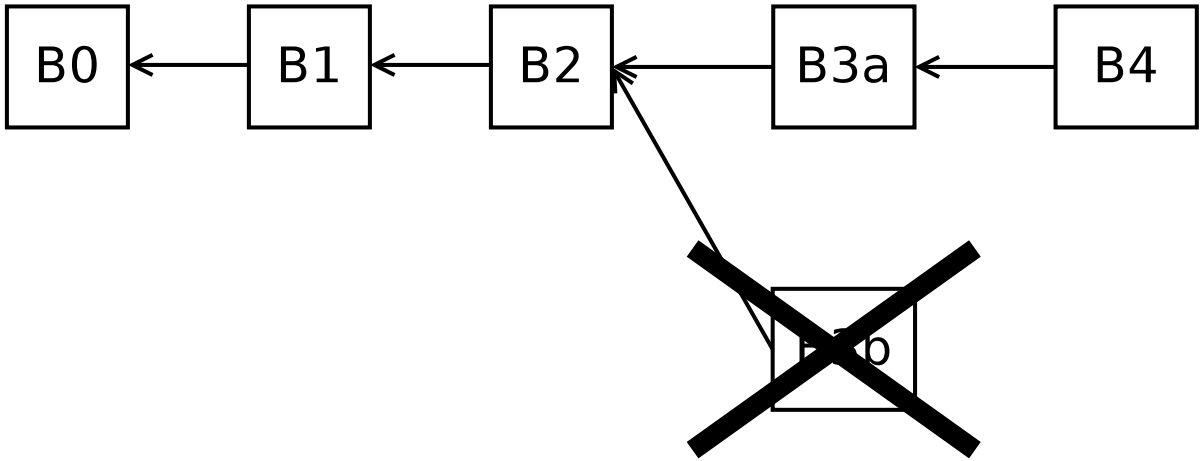




Large miner advantage

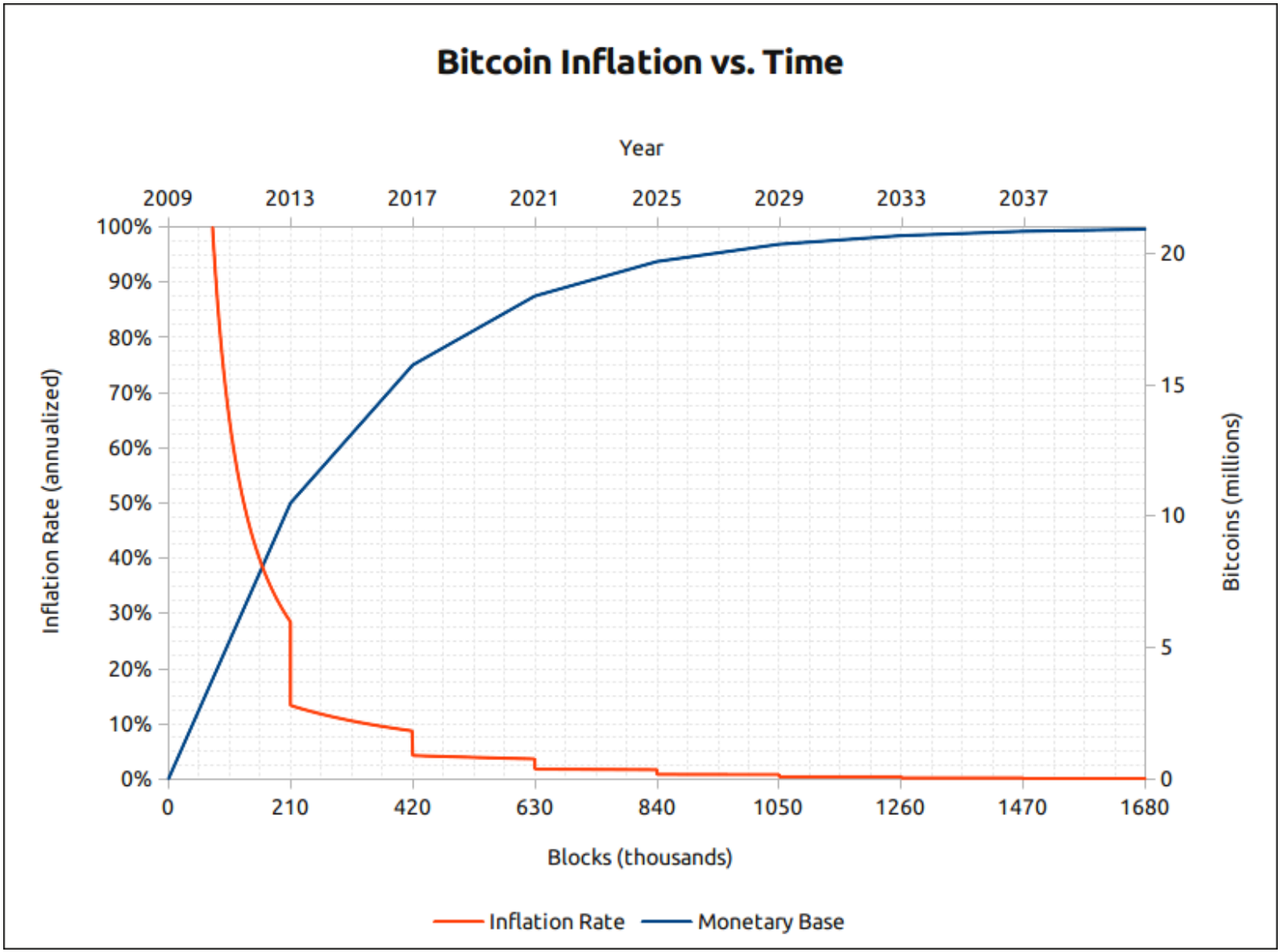


Large miner advantage



Relay network

Paying for miner security



Thank you!