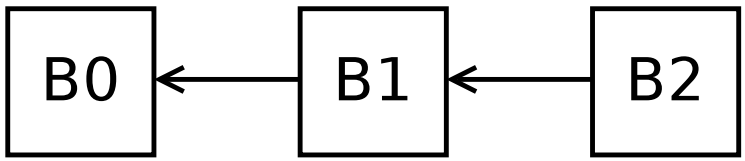
In adversarial environments, blockchains don't scale

Peter Todd

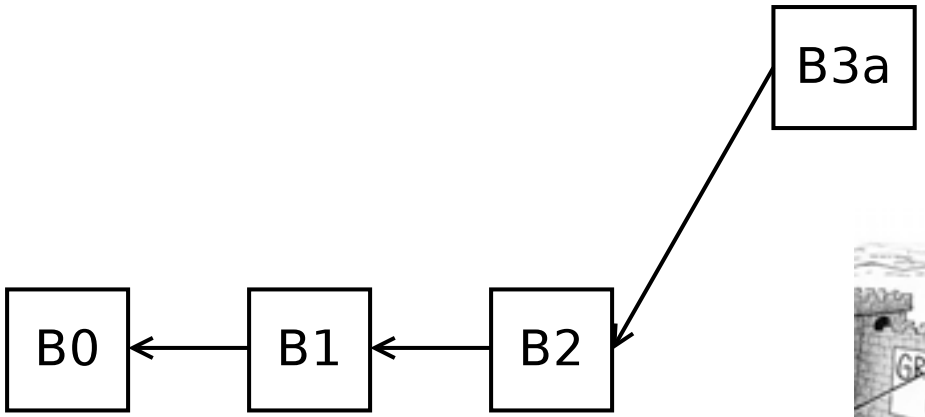
Dec 6th 2015

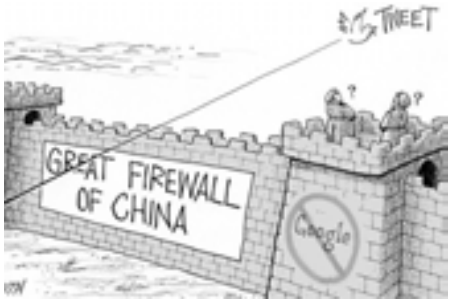
37EC 7D7B 0A21 7CDB 4B4E 007E 7FAB 1142 67E4 FA04

Large miner advantage

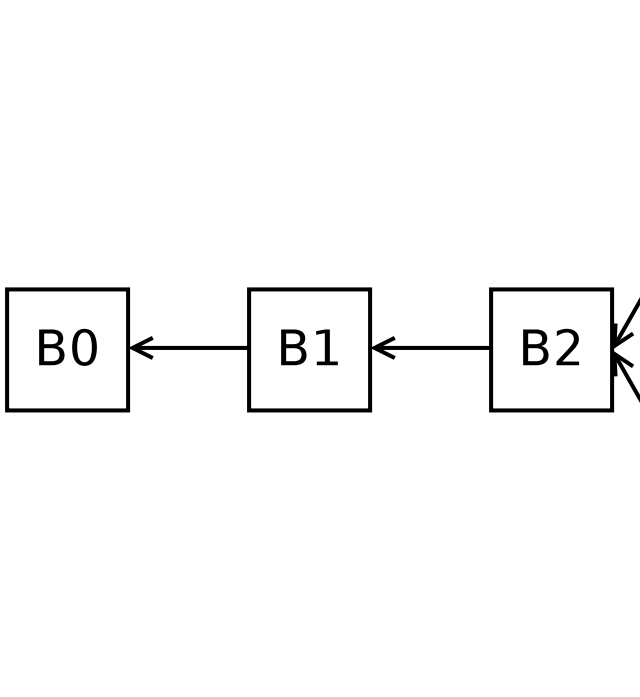


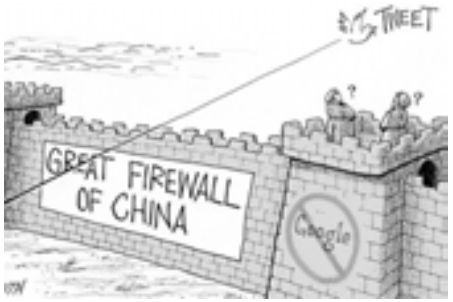
Large miner advantage



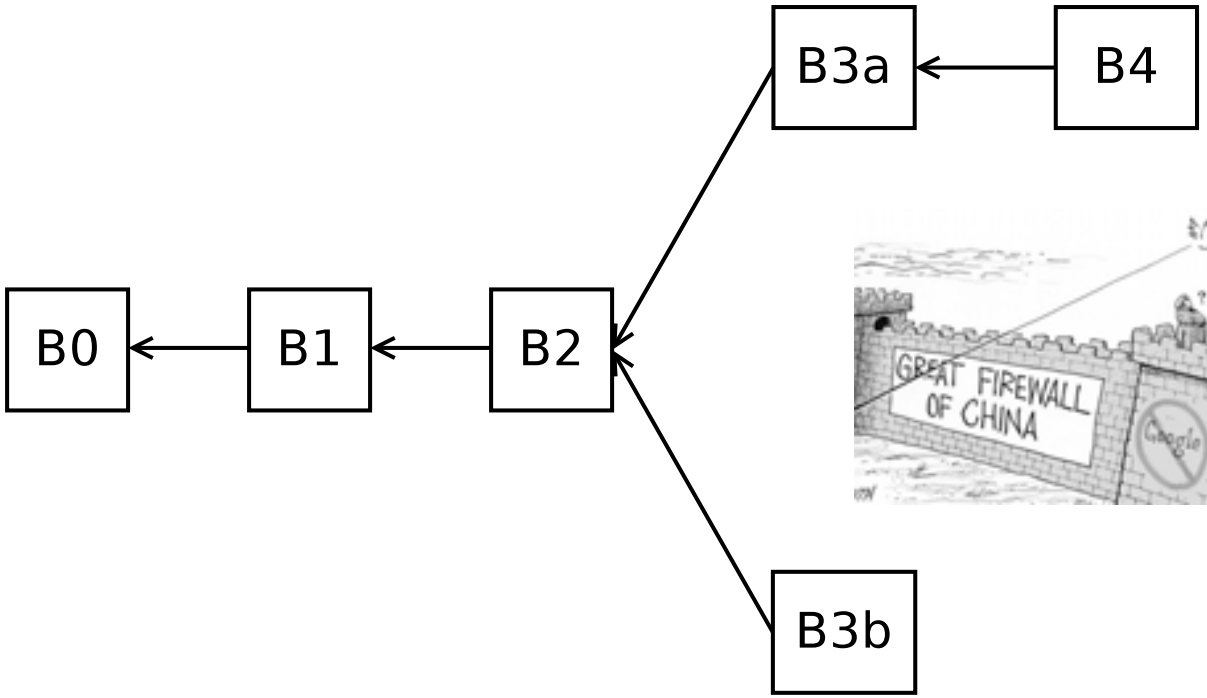


Large miner advantage

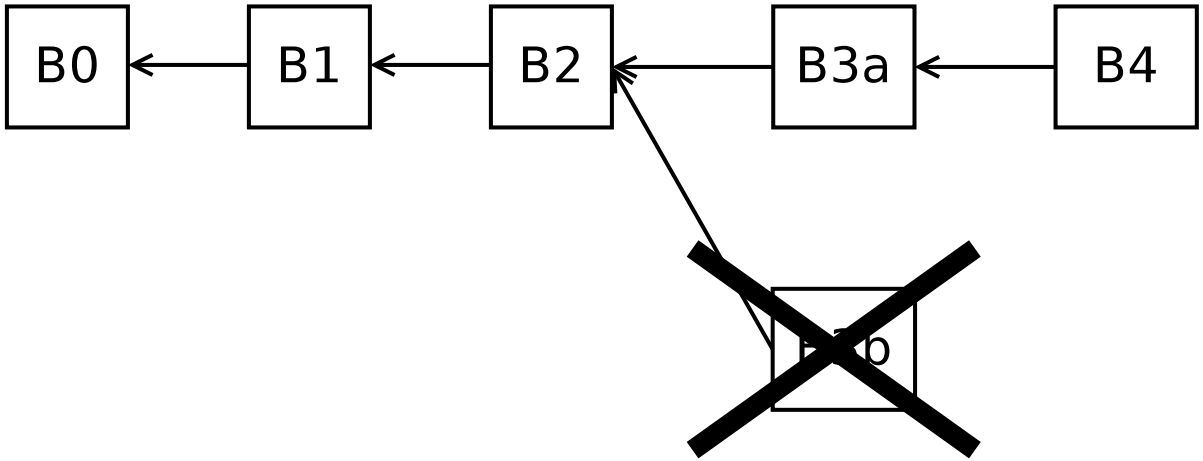




Large miner advantage

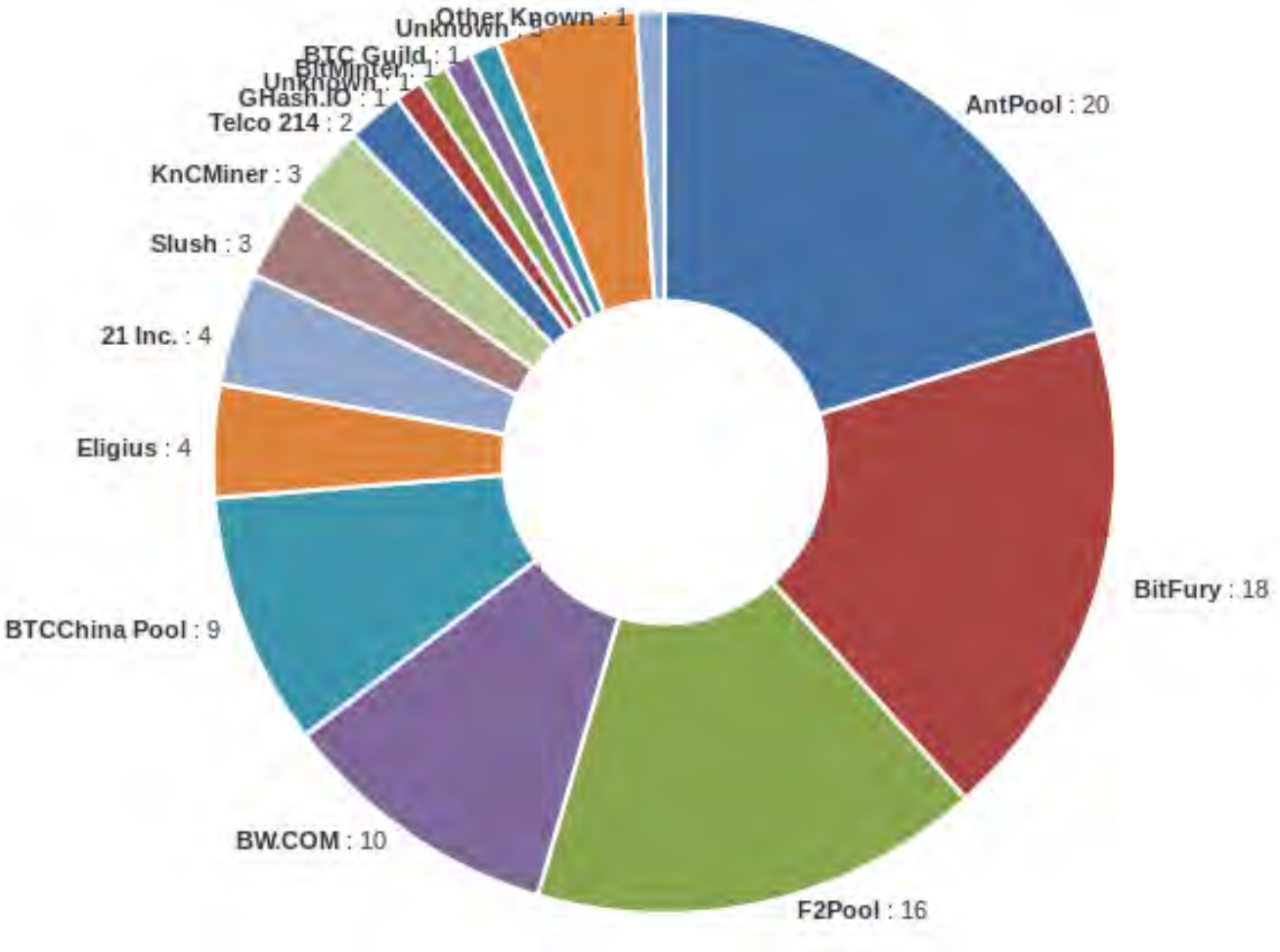


Large miner advantage

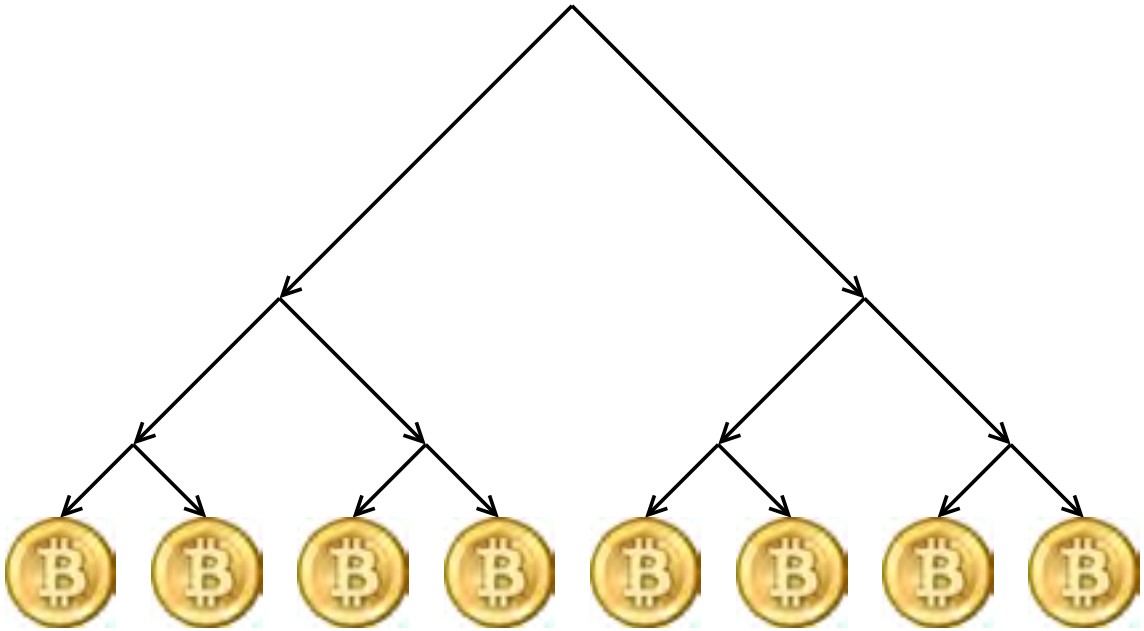


Relay network

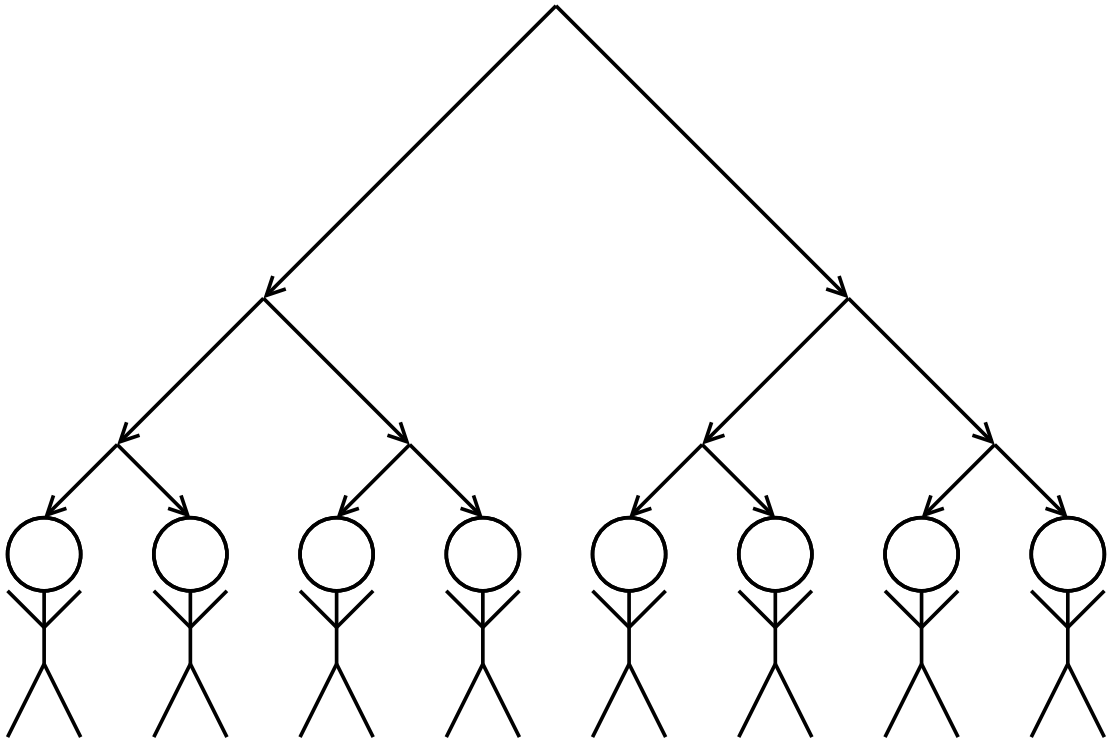
Miner centralization



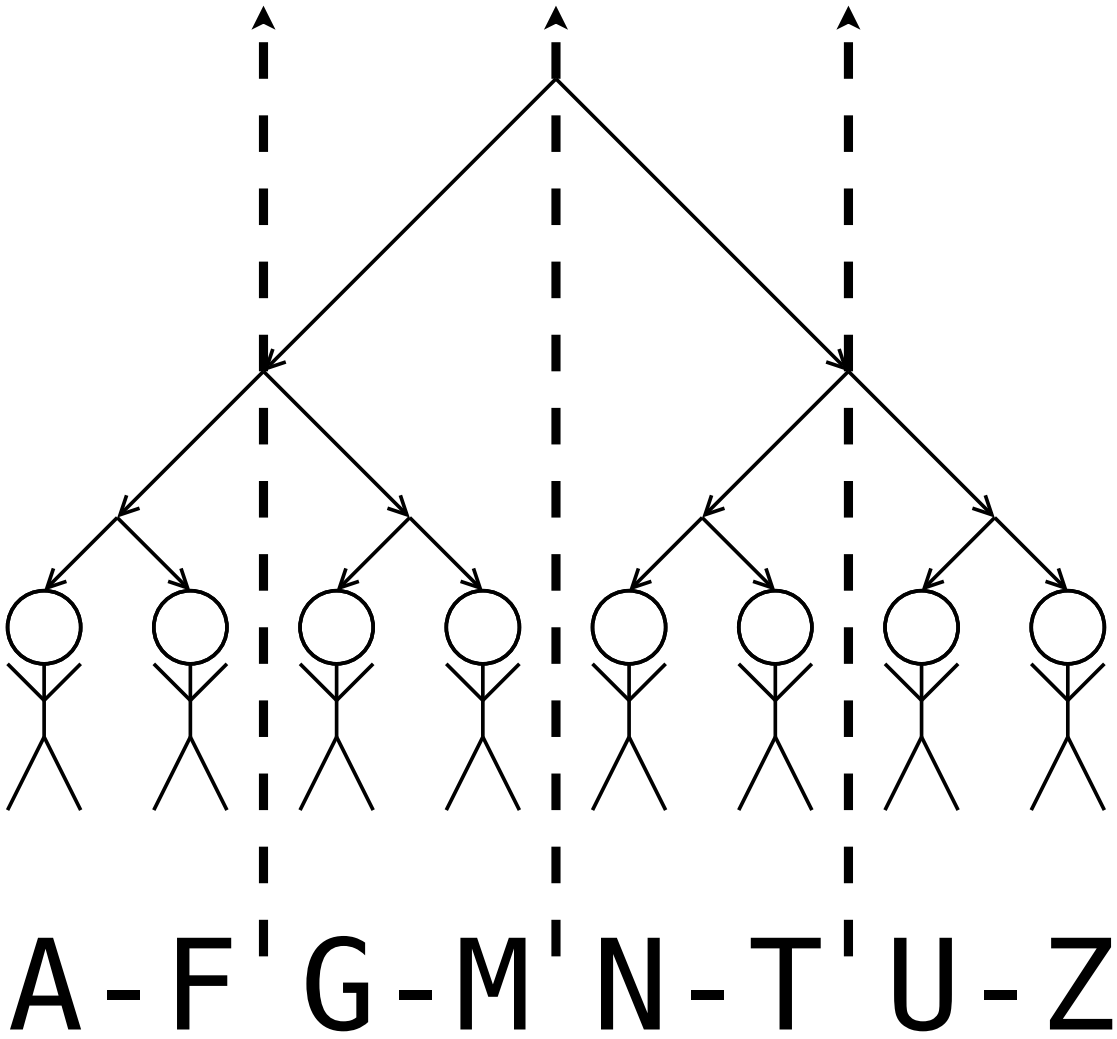
The unspent coin database



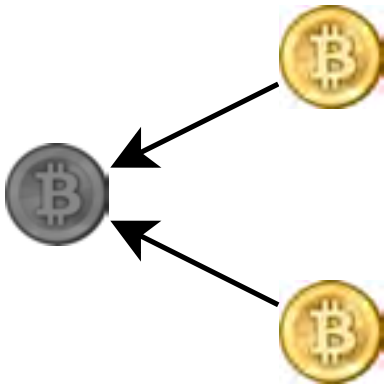
Scaling databases



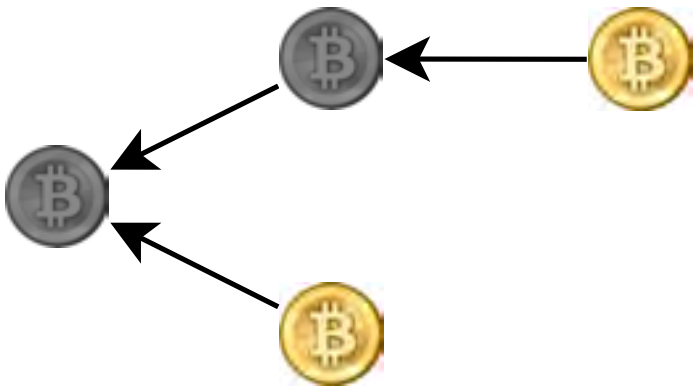
Scaling databases



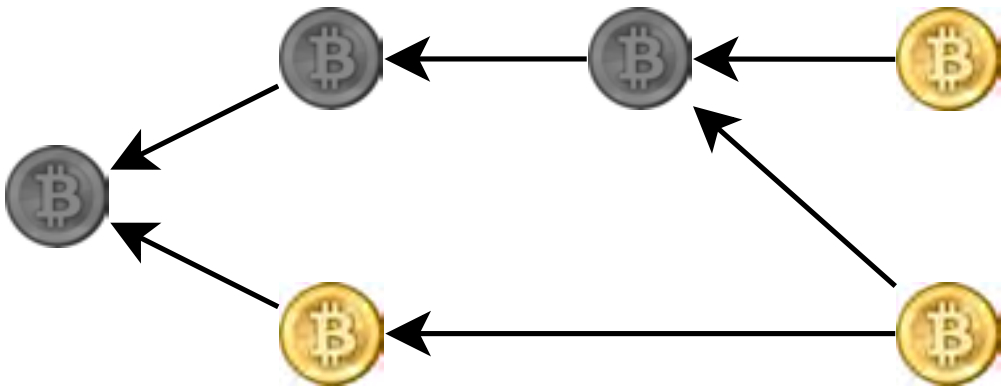
Transaction graph



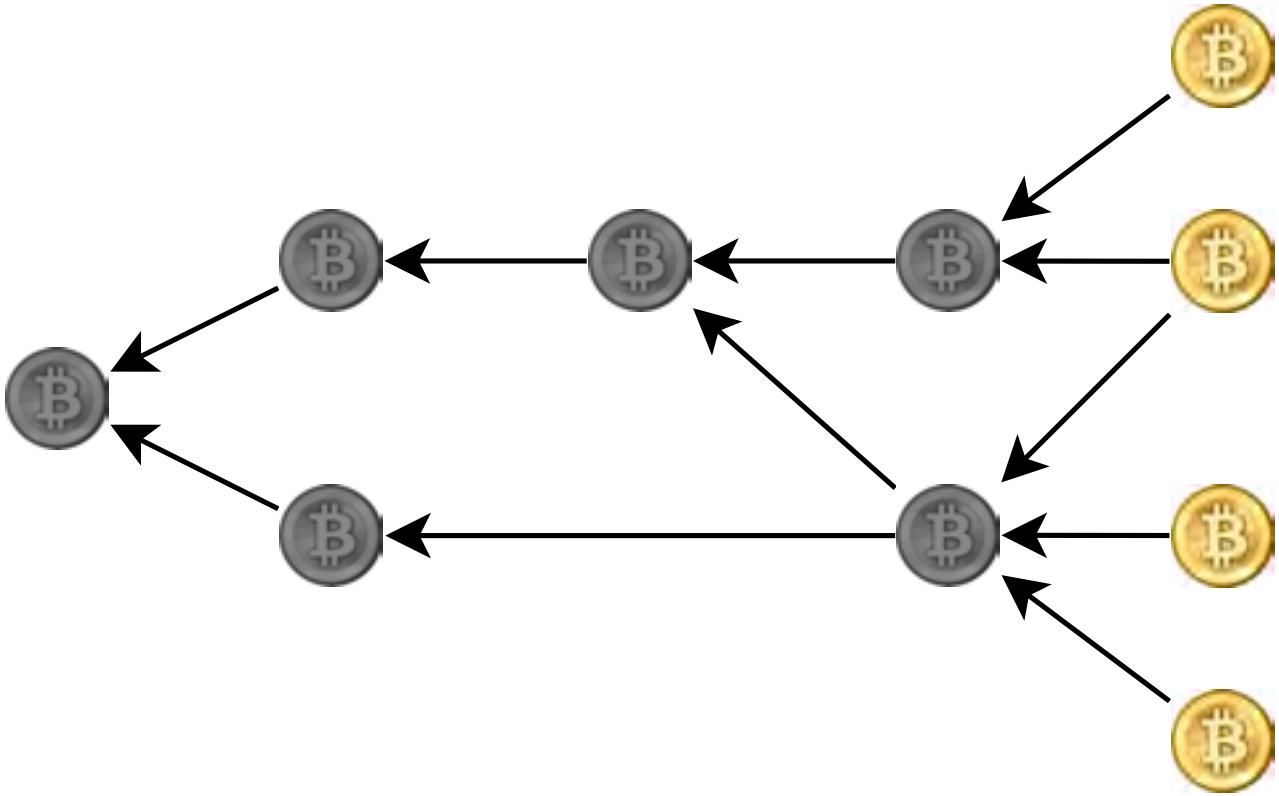
Transaction graph



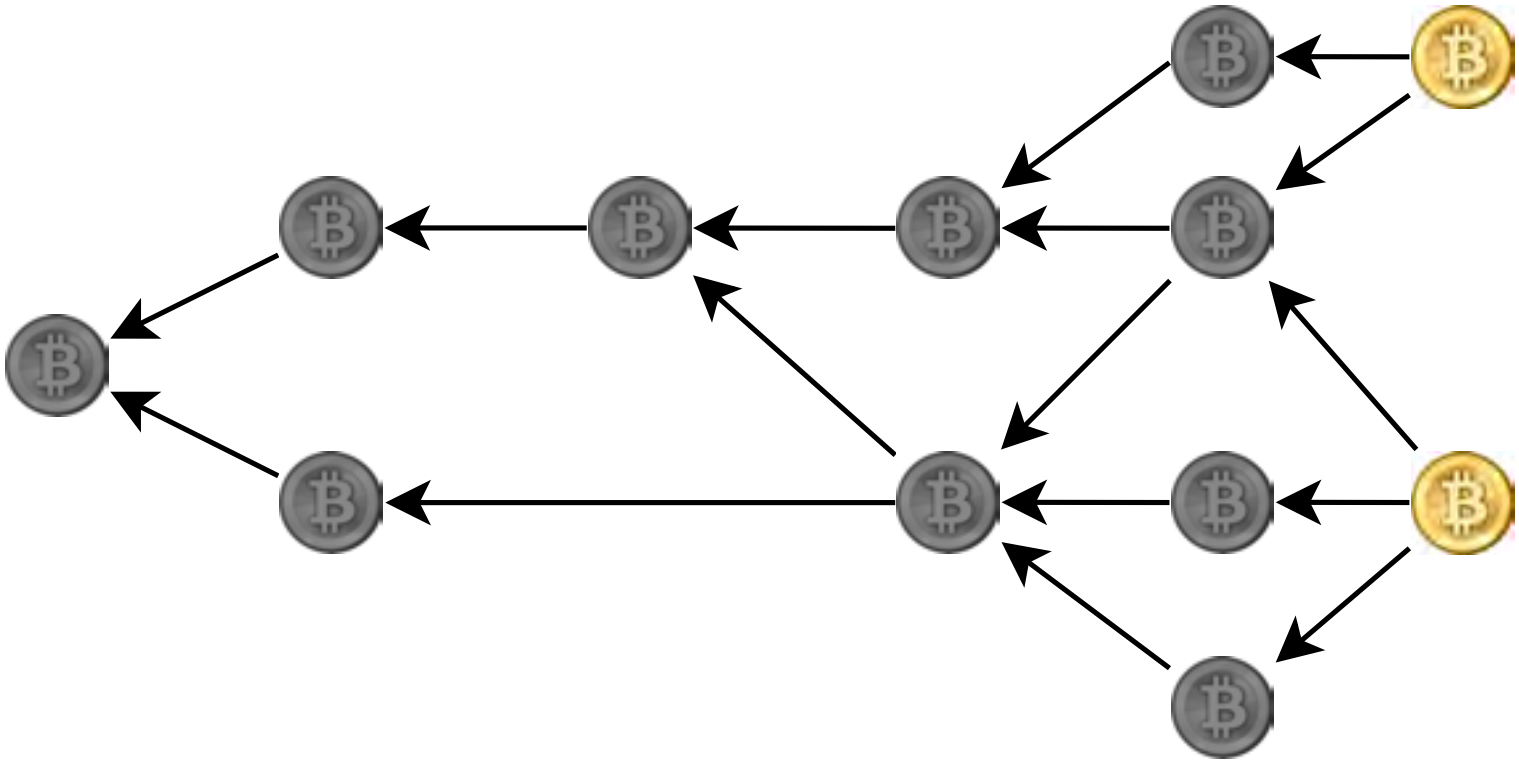
Transaction graph



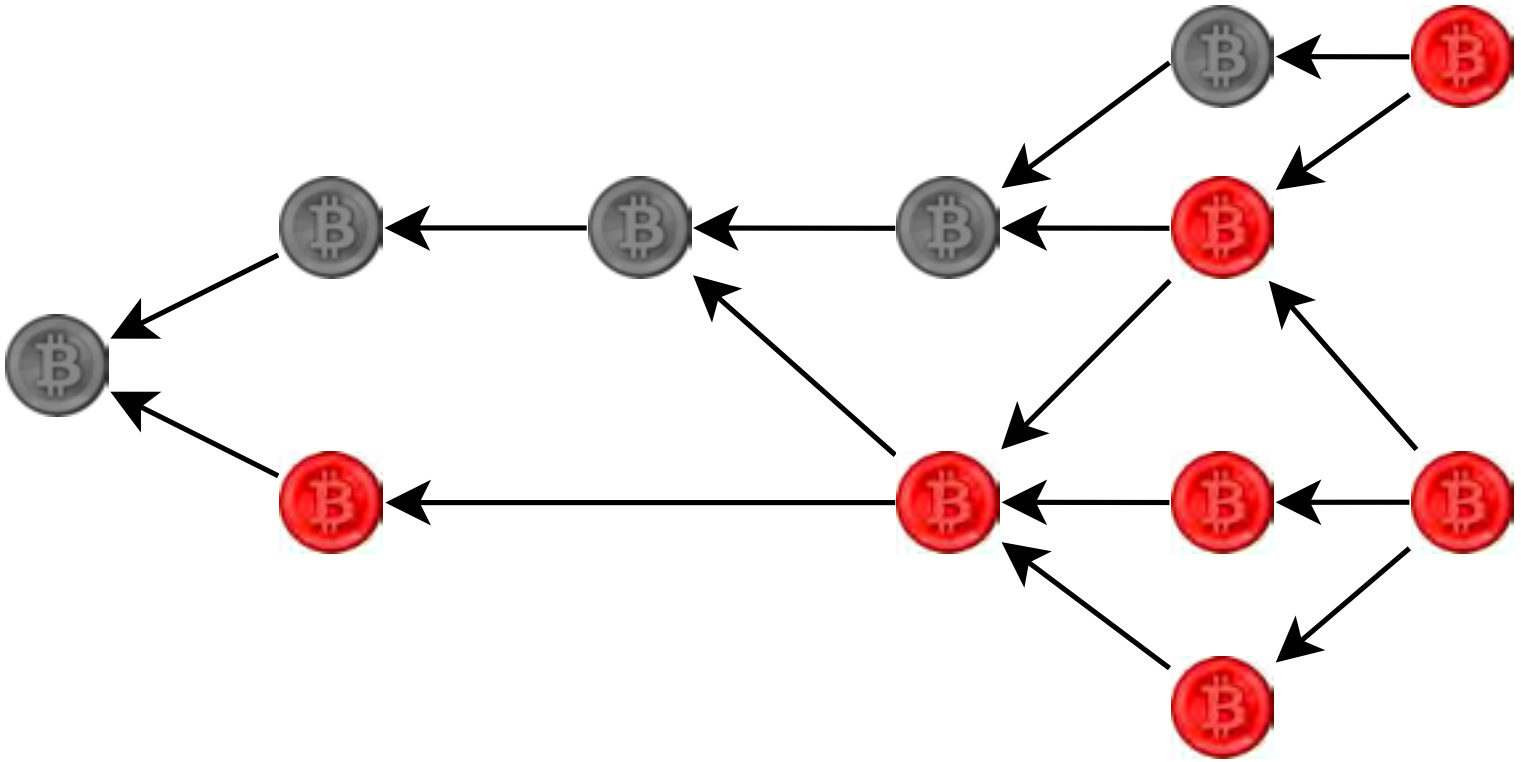
Transaction graph



Transaction graph



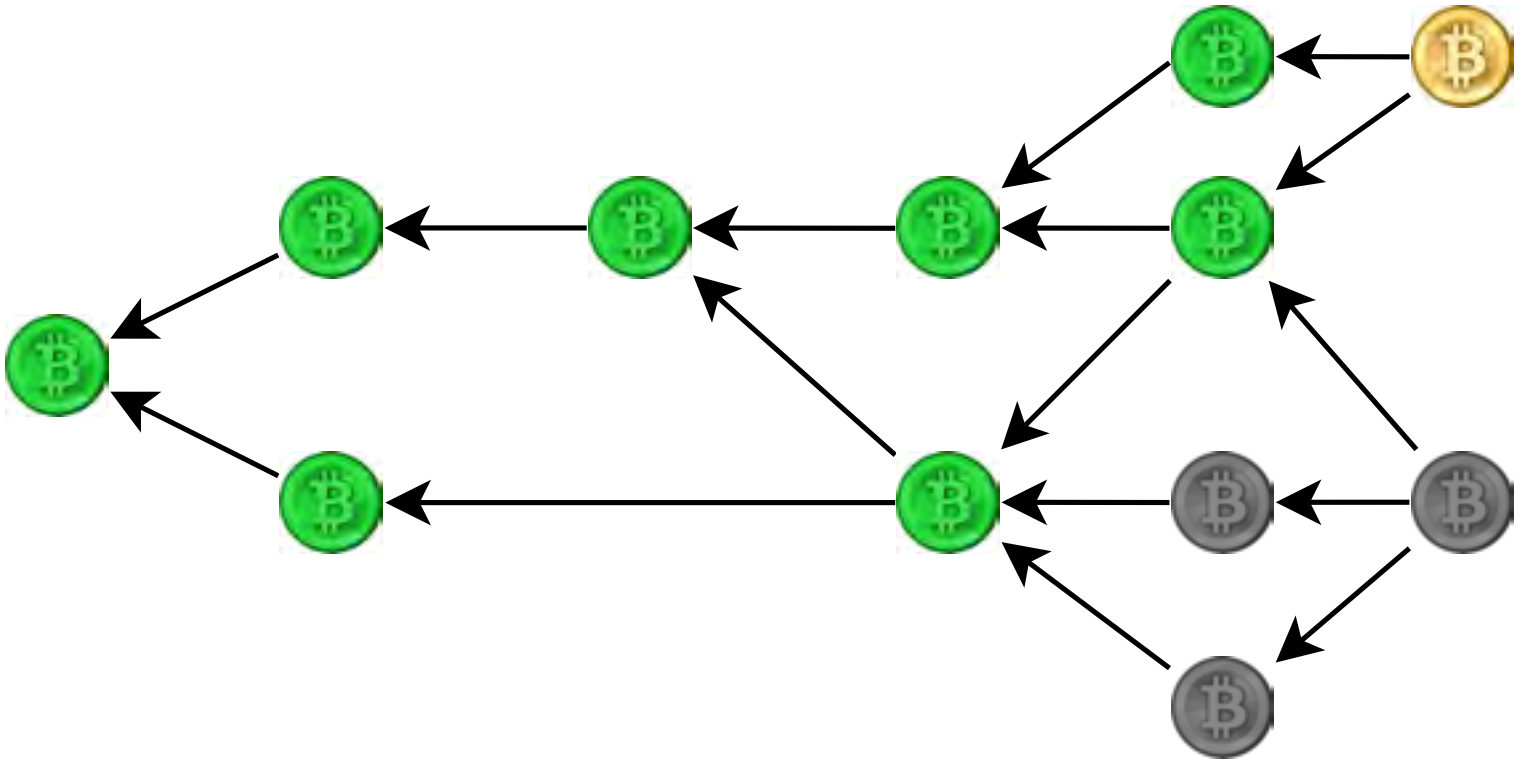
Invalid transaction graph



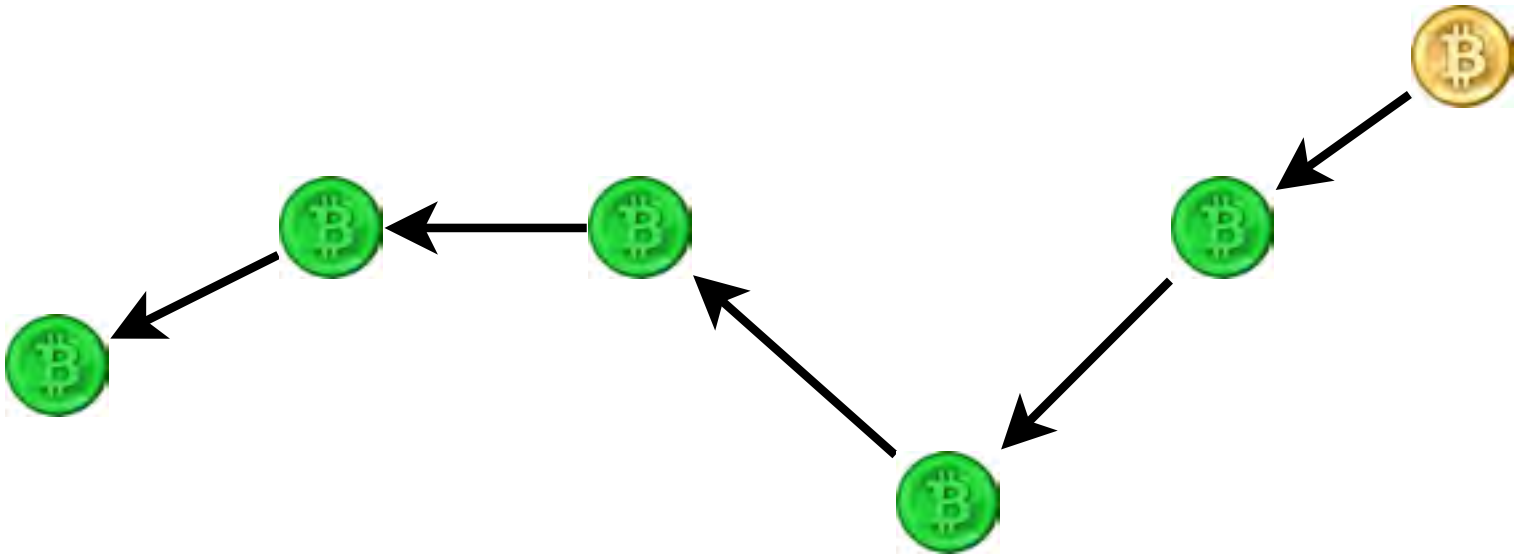
Moving forward

Solutions?

Client-side validation



Transaction history linearization



Thank you!