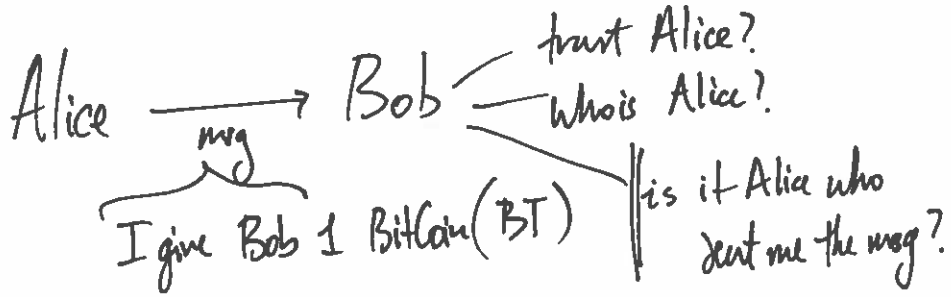
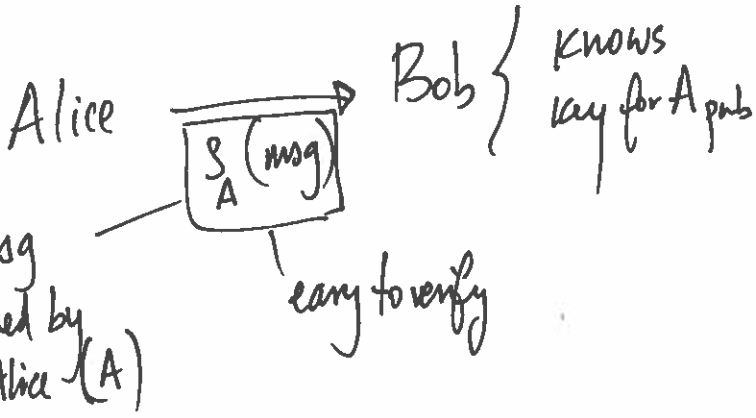
Jan 26, 2018

- × Assign 1 marks back later today
- × Assign 2 due Monday evening
- × Project 1 — find a group, register for repo (check repo exists); out next week
- × Blockchain-based
- × Today: BitCoin blockchain; background for Project 1

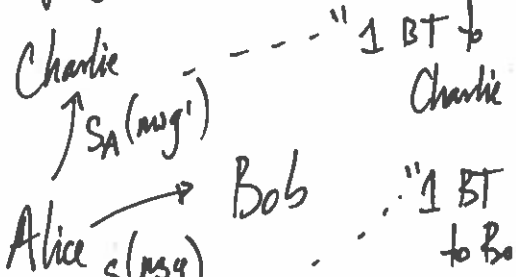
Key ideas:
- → proof of work (A1)
- → blockchain
- → P2P transactional ledger

Key challenges:
- Double spending.
- Trust in network.
- Incentives.

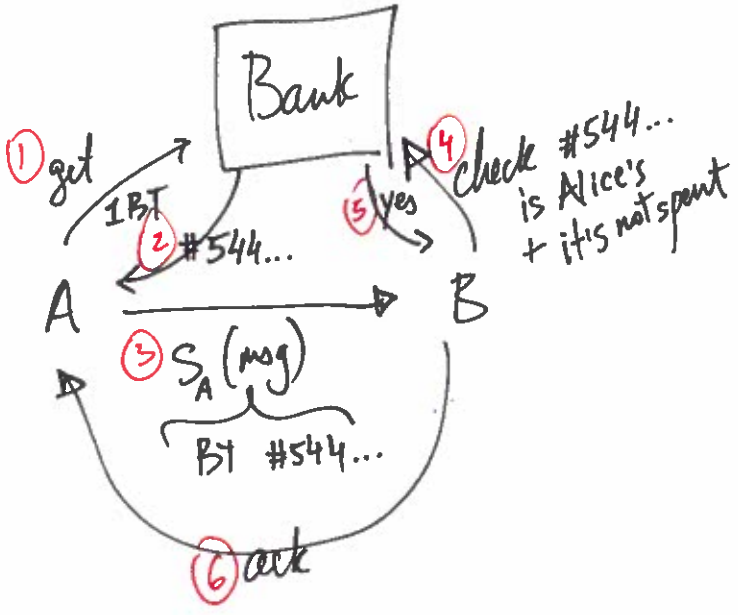


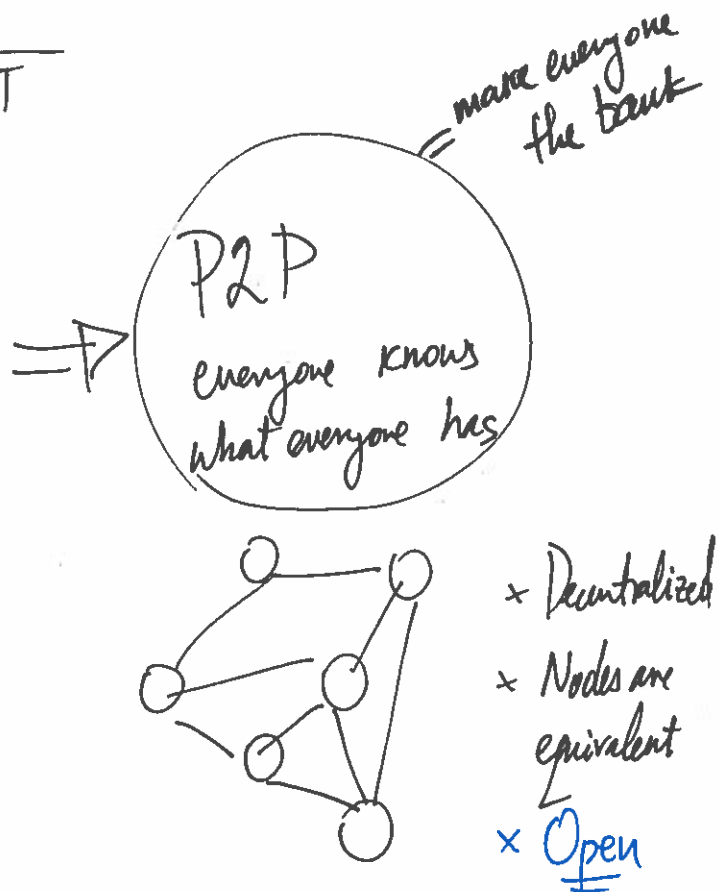


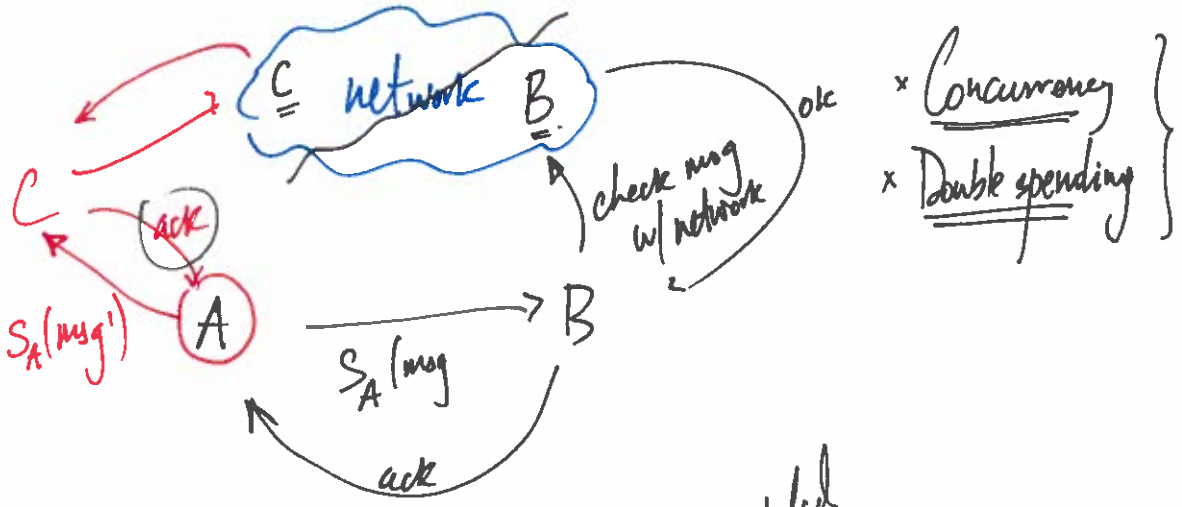
Replay attacks

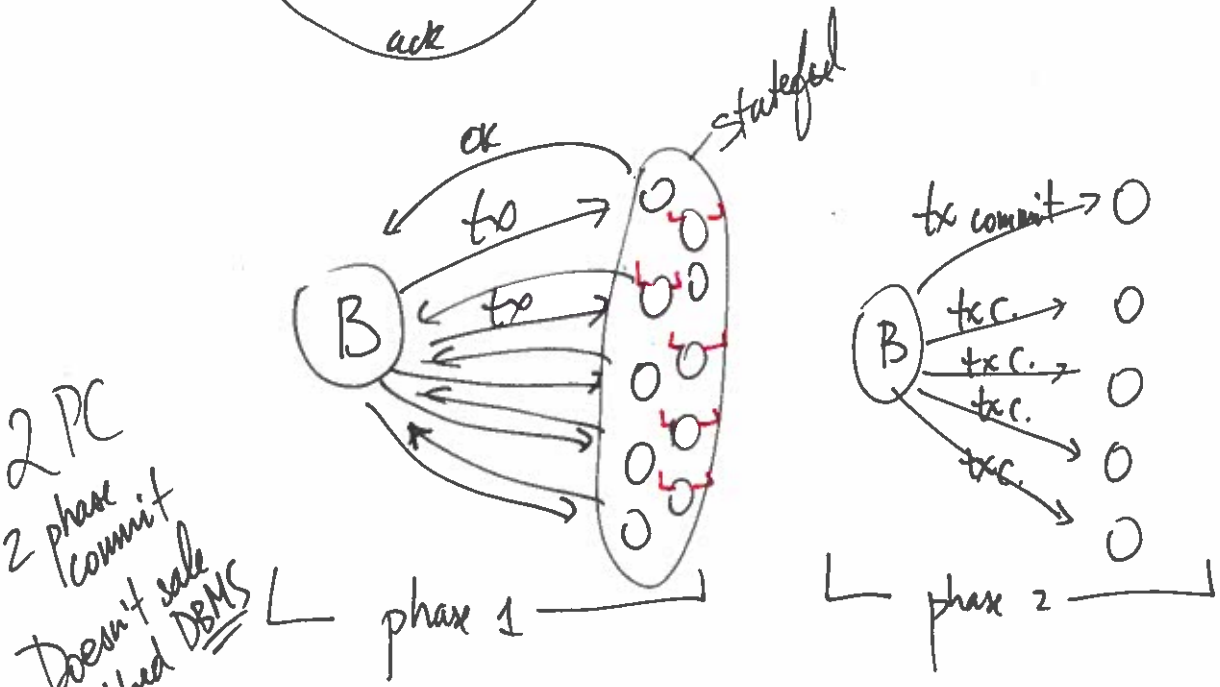


Trusted source w/ serial #s for each BT





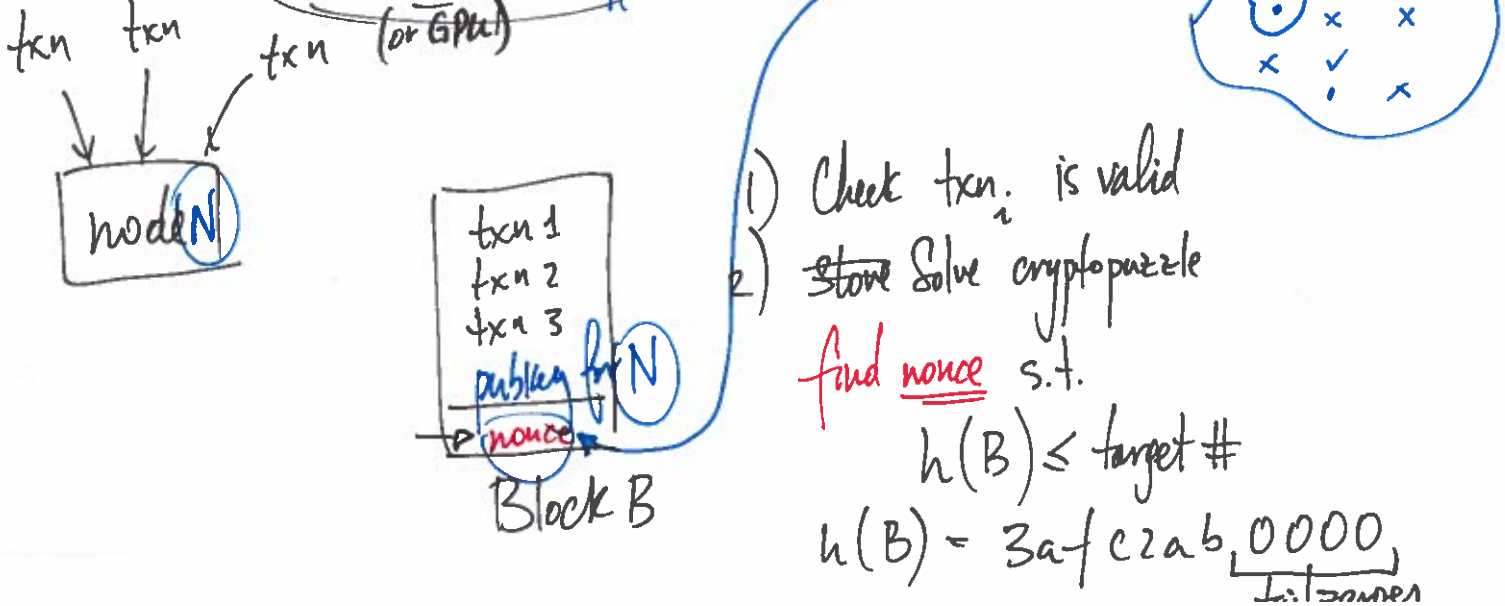


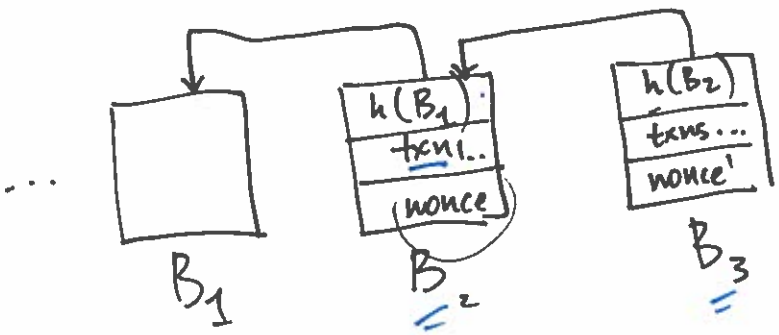


proof of work : eliminates sybils

Raw CPU power (or GPU!)

space of all nonces





gen blocks = "mining"

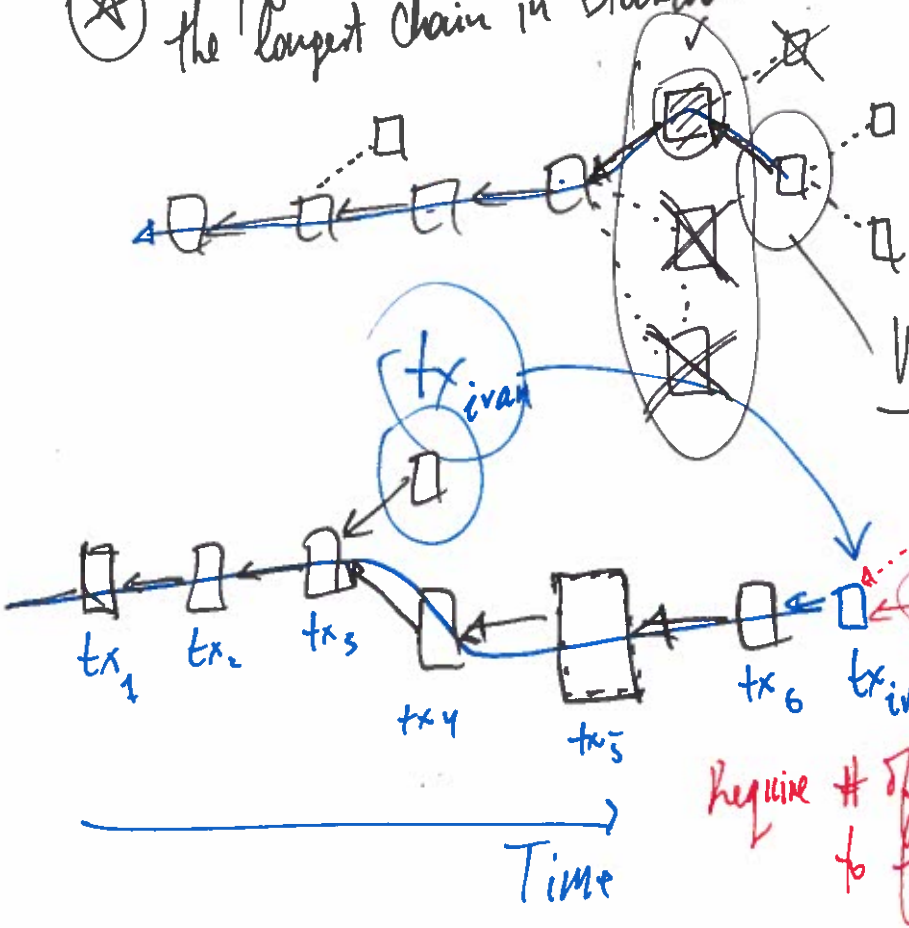
each node — validates txns

— mining

⇓

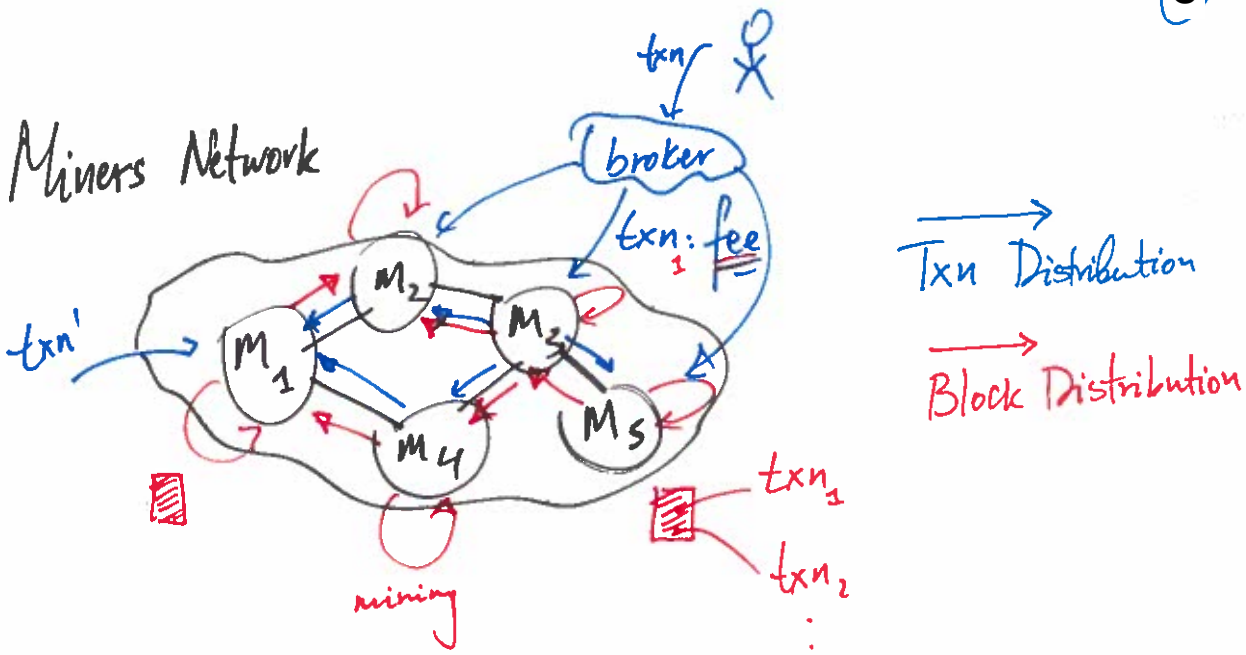
Distribute block

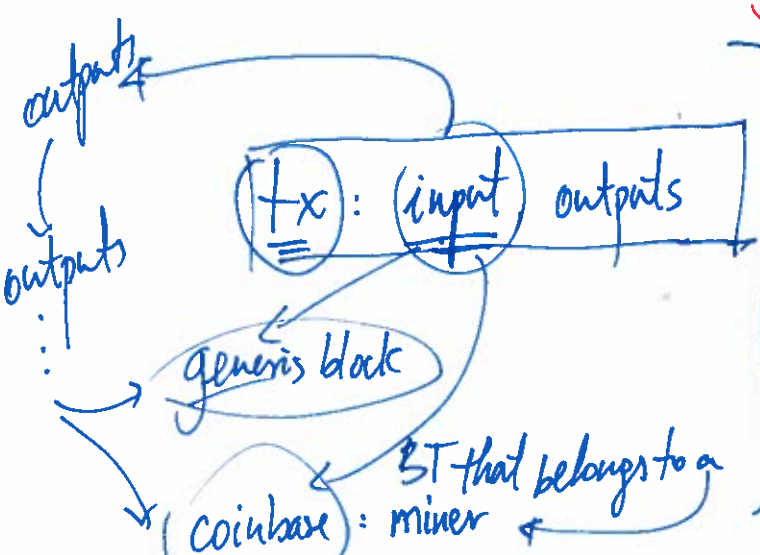
★ Only generate blocks on the Longest chain in Blockchain



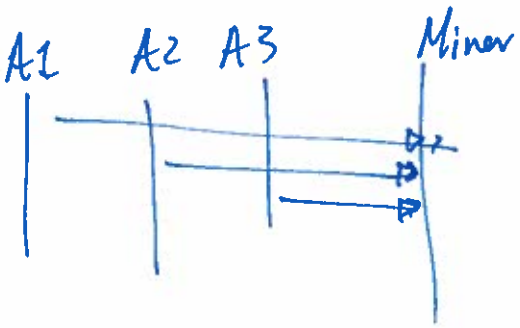
Wins: Observed + accepted by majority (CPU) of nodes

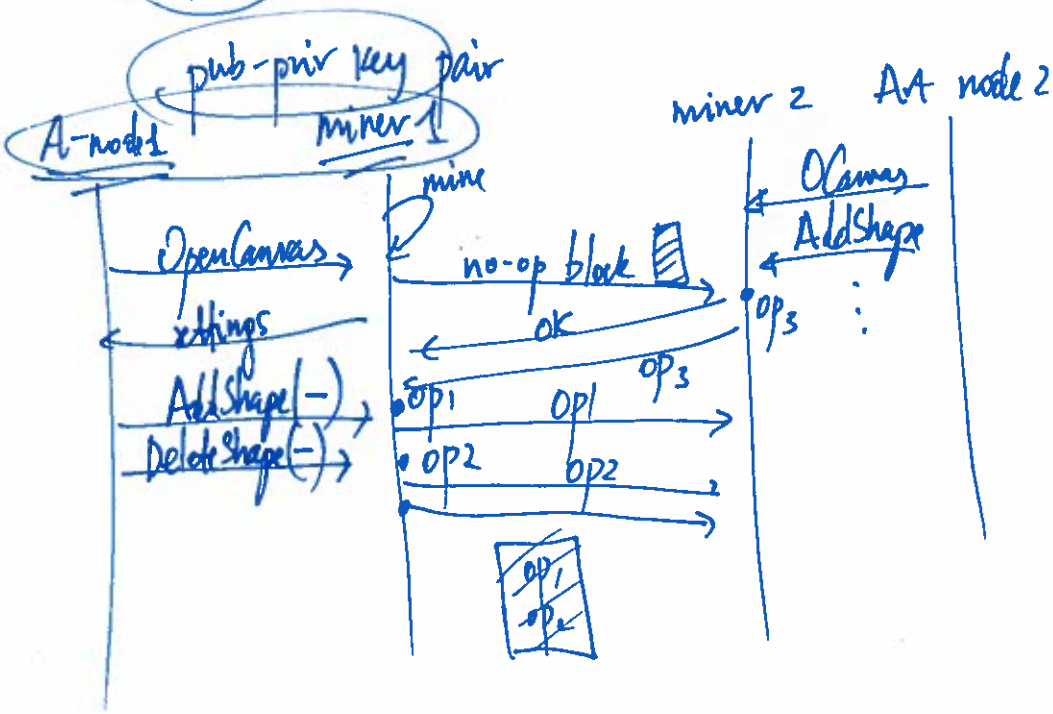
Require # of validating blocks to follow a block containing a tx.





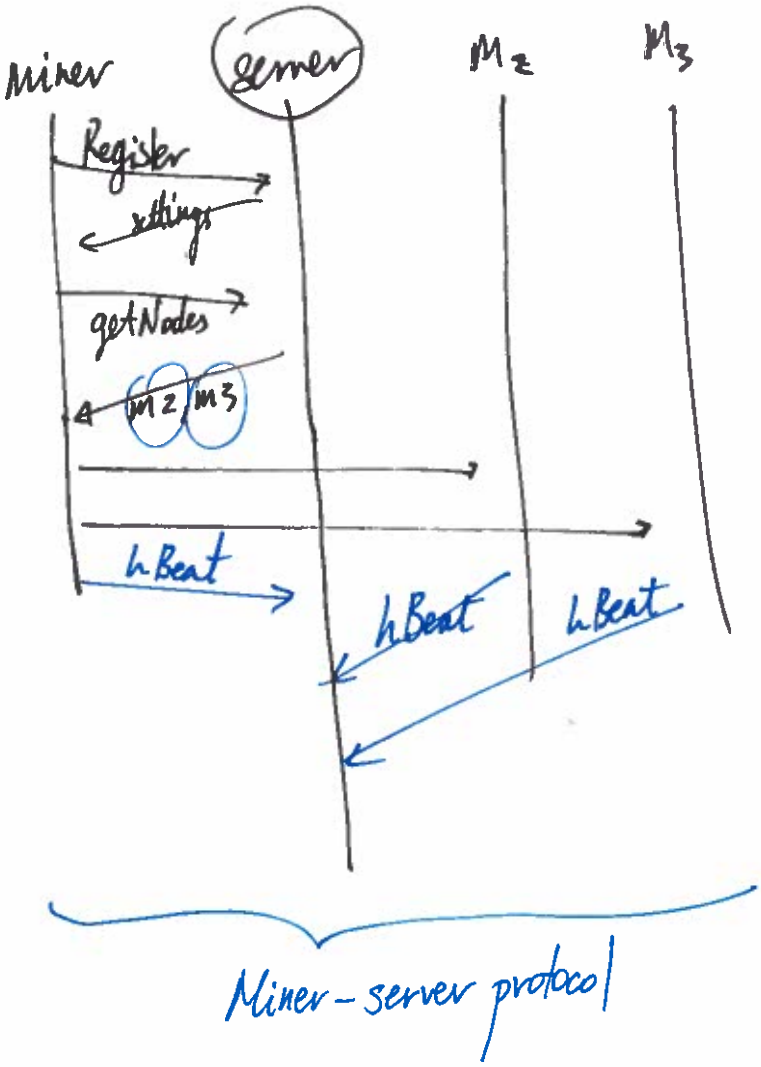
Bitcoin Does not track balances of individual accounts; only seq. of txns.





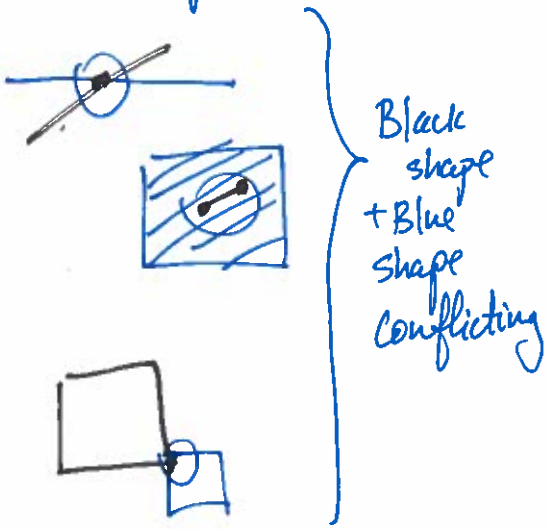
Proj 1

Art-node ↕ protocols ↕ miner ↕ miner



Miner-server protocol

Intersecting shapes ≡ conflict



Black shape + Blue shape Conflicting