CS-438 Decentralized Systems Engineering

Fall 2021

Week 13

Advanced blockchain architectures

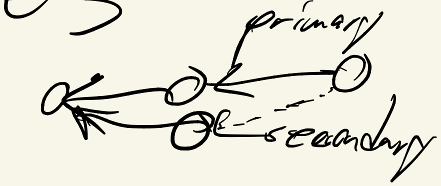
Motivation – Limitations of Bitcoin etc

- Weak finality – probabilistic, ~1 hr
- Slow – 10 mins / block
- Scalability – 1MB every 10 mins ~4 TPS
  - Ethereum: high TX fees (~25 CHF)
- Governance – upgrade, replace
- Privacy – of TX identities, amounts, data, comp.
- Bridging between chains
- Input from external world

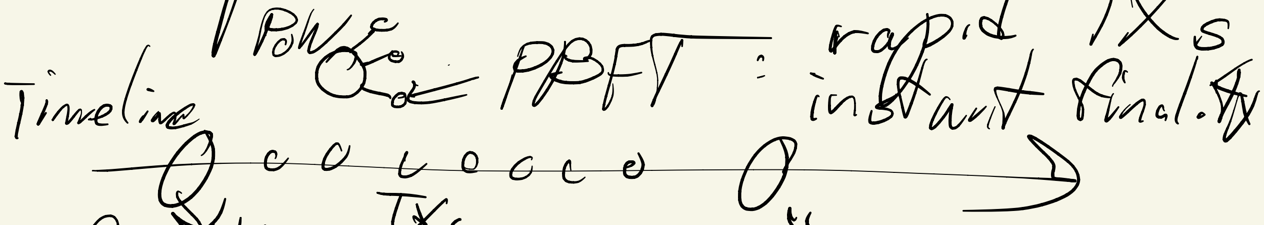
Scaling throughput / capacity

Approaches:

- More powerful nodes
- DAG-based PoW



- Sharding - OmniLedger, Ethereum
- Side-chains



Periodic summary /commitment to main chain

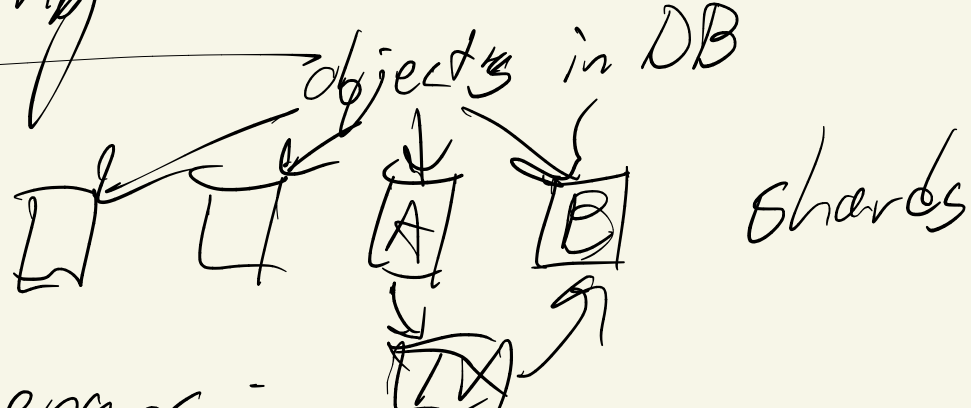
- Rollups

  checking: not just hash, but ZKP of TX history

  optimistic: claim, opportunity to challenge in period of time

- Payment channels (Lightning)

Sharding



phase 1 - lock A, B
phase 2 - apply, commit, unlock

Challenges:

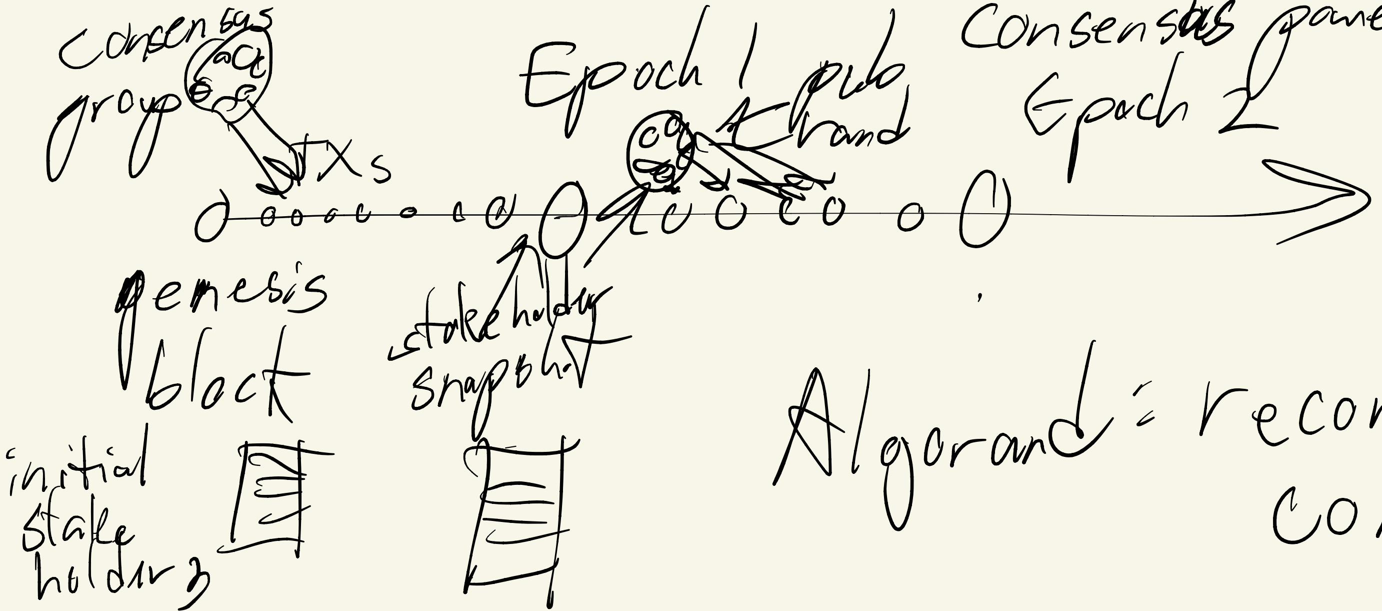
- cross-shard TXs - eg. via locking
  2-phase commit
- liveness: hanging locks? don't want to trust client
- correctness: don't want to trust any one server
  randomly-sampled subset of full nodes
  problem: attacks targeting 1 shard
  solutions: verifiable random functions (VRFs)
  Shamir secret sharing → random beacons
  RandHound, RandHerd, drand/League of Entropy

each shard - own consensus, chain

OmniLedger: 2PC on Byzantine consensus groups

Alternatives to PoW

- Proof of Burn – based on other (PoW?) chain
- Proof of Storage – Chia deployed
- PoET – "Elapsed Time" – trusted hardware
- Verifiable delay functions (VDFs) – Proof of seq. work
- ASIC-resistant PoW
- Proof of stake – buy coin, "stake" it, consensus power prop. to stake



Algorand: reconfig each consensus round