# RapidChain:Scaling Blockchain via Full Sharding

Jinghui Liao

# Outlines

- Background
- Protocol
- Evaluation
- Conclusion

# Background

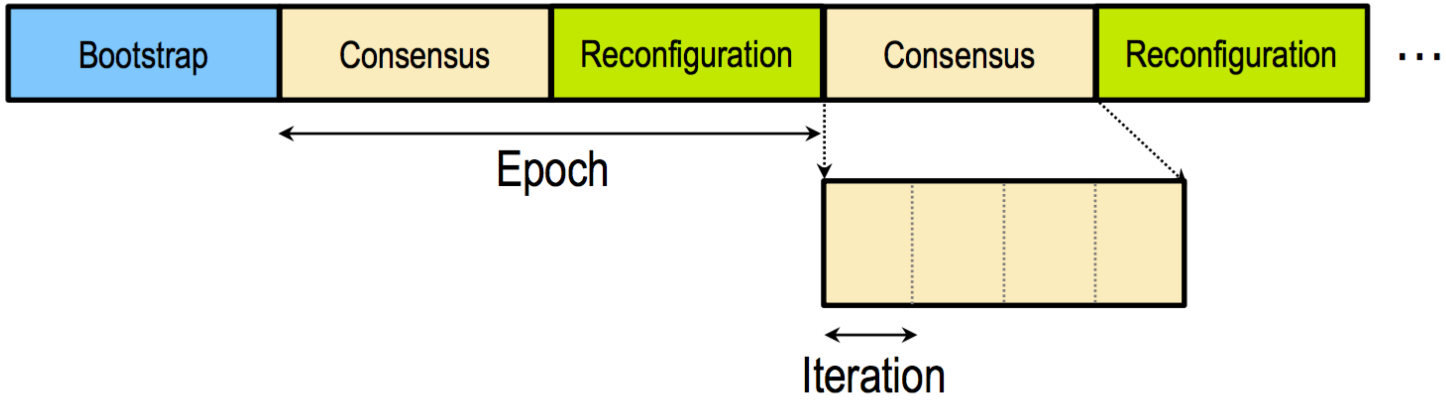
- POW and/or POS
  - Low transaction throughput
  - High latency
  - Poor energy efficiency
  - Centralization
- Committee-Based Consensus
  - Introduced to reduce the complexity of Byzantine agreement
  - Fully connected networks with only a sublinear per-node overhead
  - Only theoretically, not practically

# Background

- Algorand
  - Randomly select committee members by balance
  - Refresh committee for every consensus
  - Insecure randomness
- Sharding-based Consensus
  - RSCoin
  - Elastico
  - OmniLedger
- Synchronous Consensus
- Information Dispersal Algorithms

# Protocol

- Bootstrapping
- Consensus
- Reconfiguration



# BootsTrapping

- Root group.
  - Running committee election protocol to select a root group.
- Reference Committee
  - Root group generating a sequence of random bits to establish a reference committee
- Establish Committees
  - Reference committee are responsible to create committees

# Consensus

- Gossip
  - Divides M into k chunks M1 M2 M3….Mk
  - Give chunks to neighbors equally
  - Message should be able to be reconstructed
- Remarks Synchronous Consensus
  - Run on small number of nodes
  - Size of message to agree is small
  - Latency of each round of consensus is also small
  - High resiliency (1/2)

# Consensus

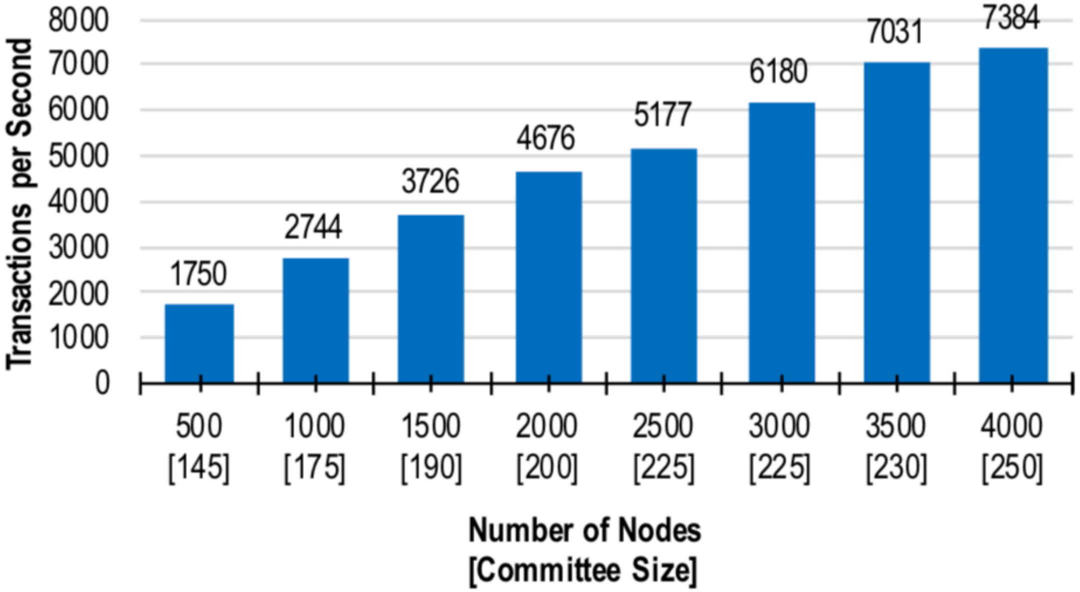
- Cross-Shard Transaction
  - Each tx has a unique identity
  - If the input is unspent
  - If the sum of outputs is less than the inputs
  - Transactions are partitioned based on tx id.
  - No proof attached to tx
  - On cross shard transaction will be split into 3

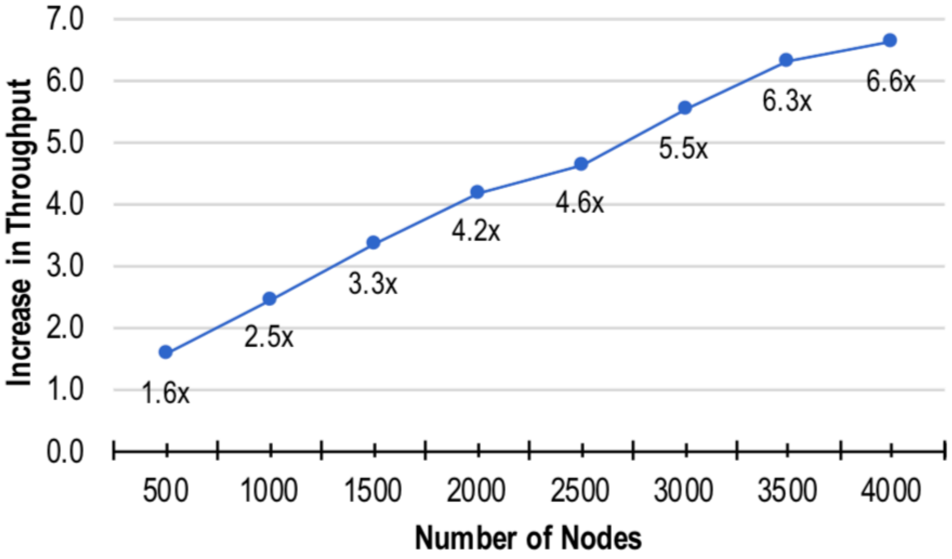
# Reconfiguration

- Offline PoW
  - Rely on Pow to protect against Sybil
  - Reference committee is responsible to verify  PoW result
- Randomness Generation
  - Reference Committee run a Distributed random generation protocol
- Cukoo Rule
  - Randomly assign new node
  - Assign a number of members in the committee to another committee

# Evaluation

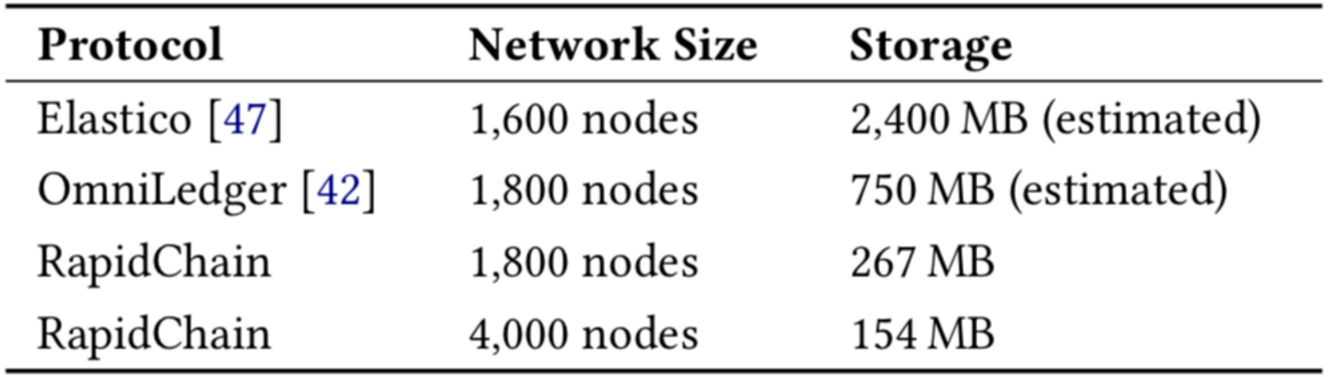
- Committee Size





# Evaluation

- Storage



| Protocol | Network Size | Storage |
|---|---|---|
| Elastico [47] | 1,600 nodes | 2,400 MB (estimated) |
| OmniLedger [42] | 1,800 nodes | 750 MB (estimated) |
| RapidChain | 1,800 nodes | 267 MB |
| RapidChain | 4,000 nodes | 154 MB |

# Conclusion

- 1/3 resilient sharding-based blockchain protocol
- Highly scalable
- Committee based network and storage
- Scales smoothly to the size up to 4000 nodes

Thank you!