



UCDAVIS

RESILIENT CONSENSUS SUSTAINED COLLABORATIVELY

Mohammad Sadoghi

Coinbase Machine Learning and Blockchain Research Summit

May 5, 2023



Mohammad Sadoghi
Exploratory Systems Lab
Department of Computer Science
UCDAVIS
UNIVERSITY OF CALIFORNIA

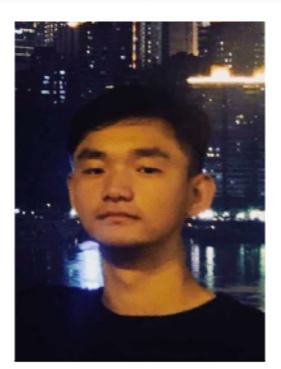




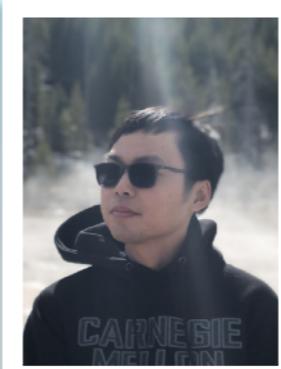
ExpoLab Team



Mohammad Sadoghi
(Principal Investigator)



Dakai Kang, PhD
(View-change-less Protocols)



Junchao Chen, PhD
(Hybrid BFT Protocols)



Shesha Vishnu Prasad, MSc **Jinxiao Yu, MSc**
(Resilient Wallet) (Performance Analyst)



Wayne Wang, MSc
(Global Consensus)



Kaustubh Shete, Mac Apratim Shukla, MSc
(Resilient NFT) (Resilient Wallet)



Glenn Chen, BSc
(System Storage)



Julieta Duarte, BSc
(System Storage)



Divjeet Singh Jas, MSc
(dApp Developer)



Arindaam Roy, Mac
(Toolkit & Integration)



Priyal Soni, MSc
(Resilient Debitable)



Gopal Nambiar, MSc
(Full Stack Developer)



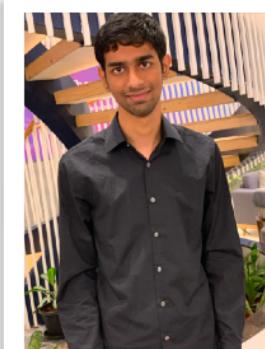
Steve Chen, BSc
(Resilient Wallet)



Haskell Lark Macaraig, BSc **Jared Givens, BSc** **Saipranav Kotamreddy, BSc**
(Concurrency Control) (Concurrency Control) (Concurrency Control)



Shubham Pandey, MSc
(Scaling Fabric via RDMA)



Rohan Sogani, MSc
(Scaling Fabric via Sharding)



Jelle Hellings, PostDoc
(Fault-tolerant Complexity)



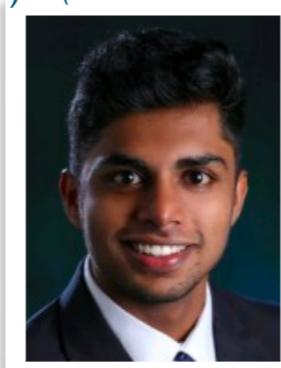
Suyash Gupta, PhD
(Scalable Consensus)



Sajjad Rahnama, PhD
(Global Consensus)



Thamir Qadah, PhD
(Coordination-free Concurrency)



Dhruv Krishnan, MSc
(Scaling Fabric via Sharding)



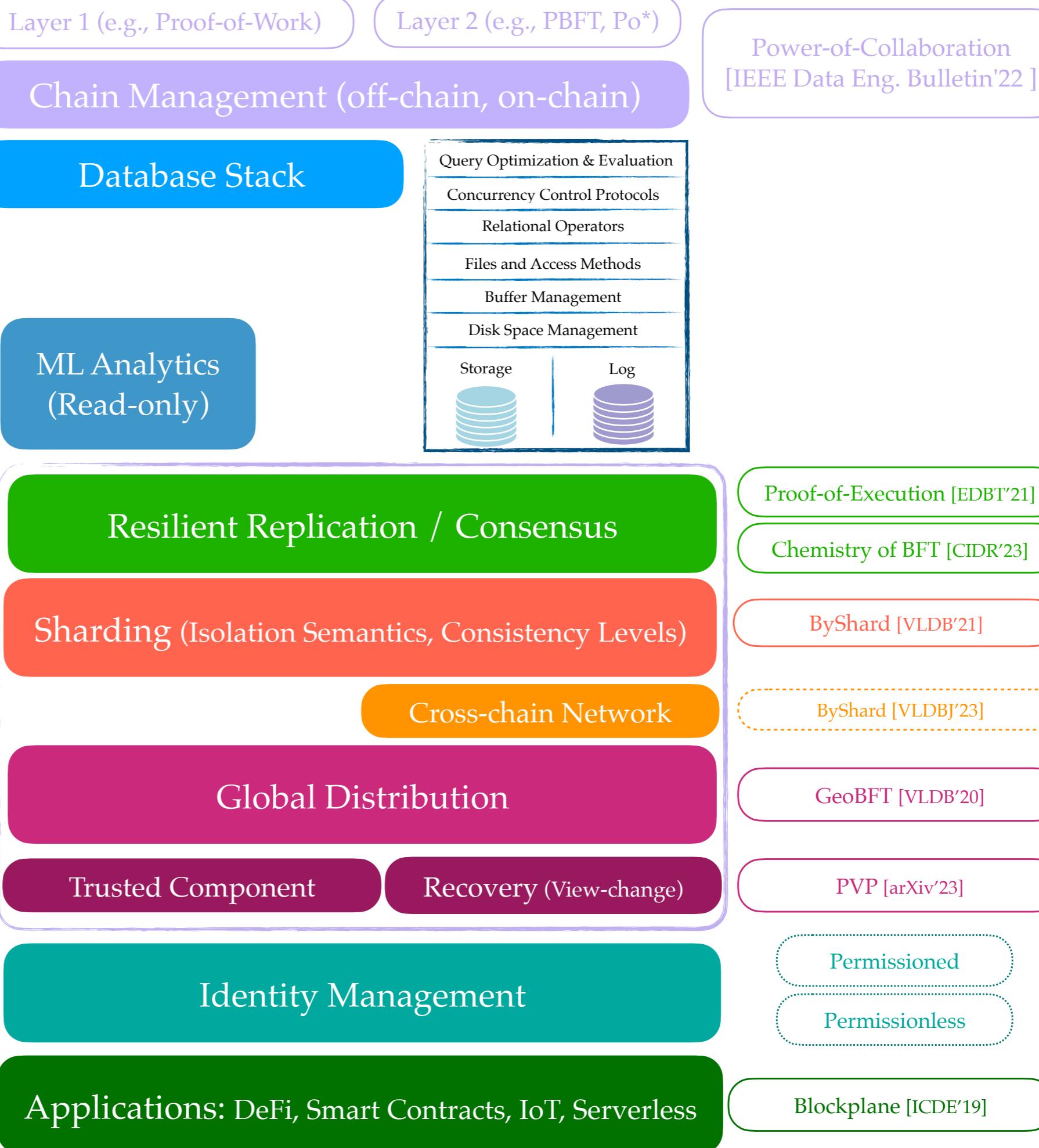
Priya Holani, MSc
(Scaling Fabric via Sharding)

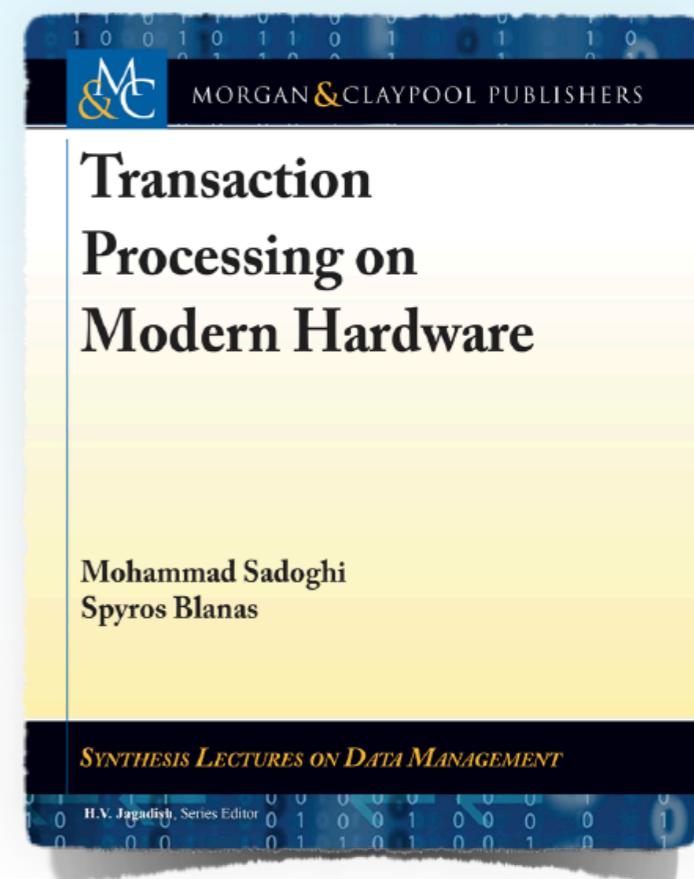
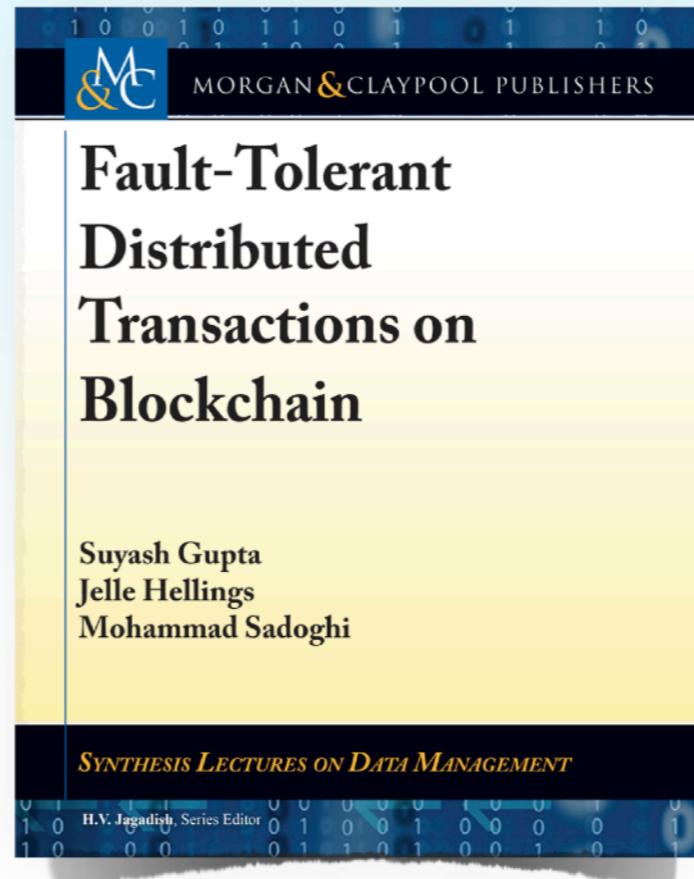
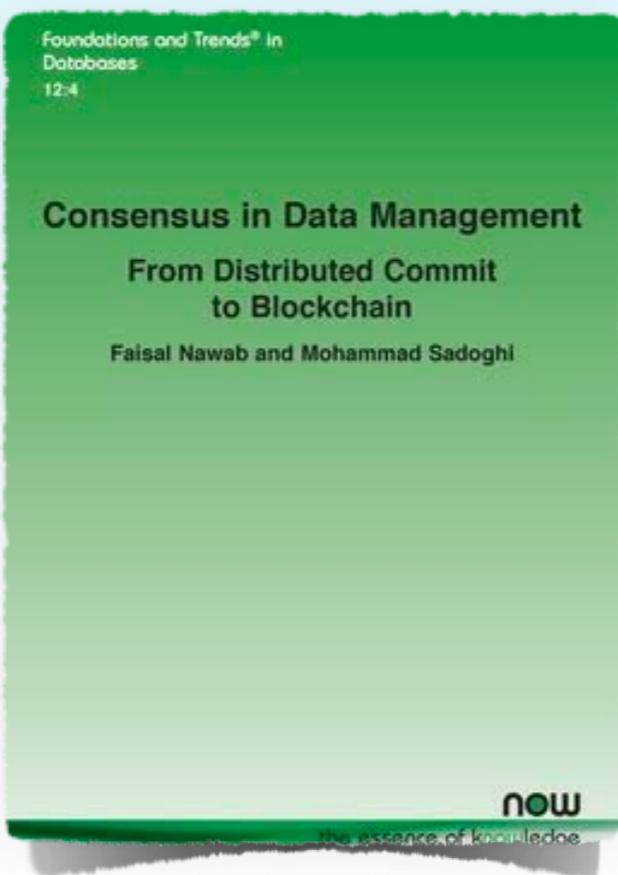


Shubham Pandey, MSc
(Scaling Fabric via RDMA)



Rohan Sogani, MSc
(Scaling Fabric via Sharding)





Books

[Consensus in Data Management: From Distributed Commit to Blockchain.](#)
Foundations and Trends® in Databases. Now Publisher. 2023

Fault-Tolerant Distributed Transactions on Blockchain.

Synthesis Lectures on Data Management, Morgan & Claypool / Springer Publisher. 2021

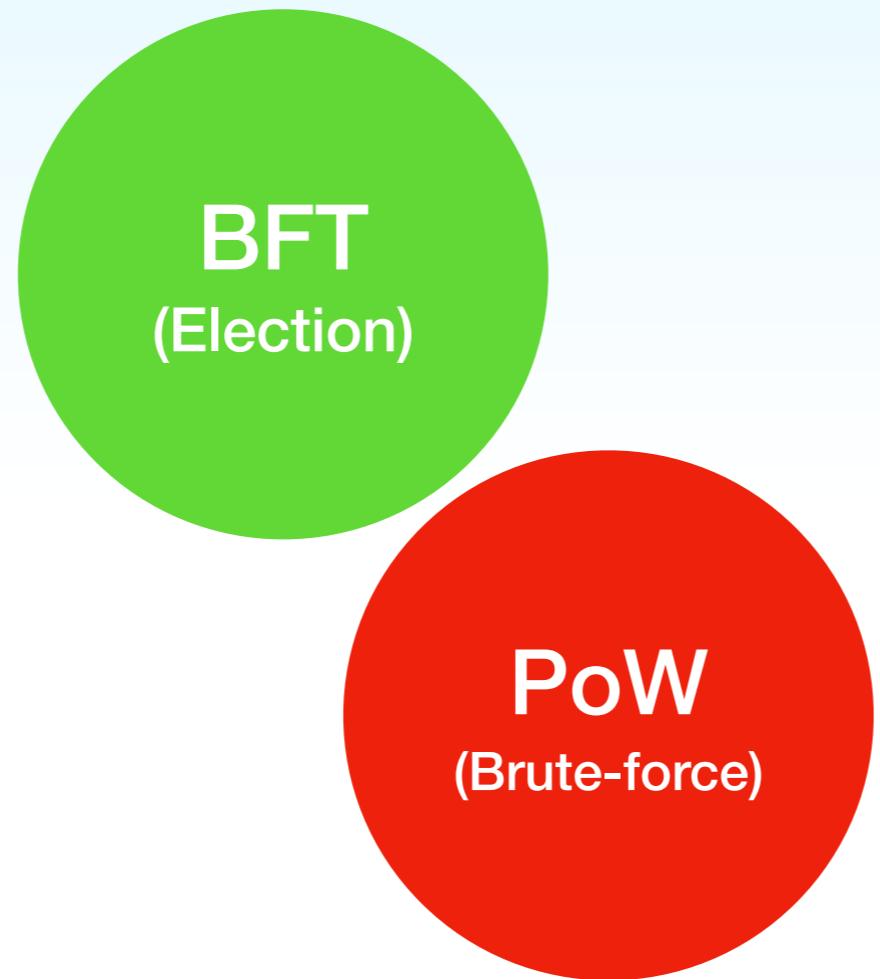
Transaction Processing on Modern Hardware.

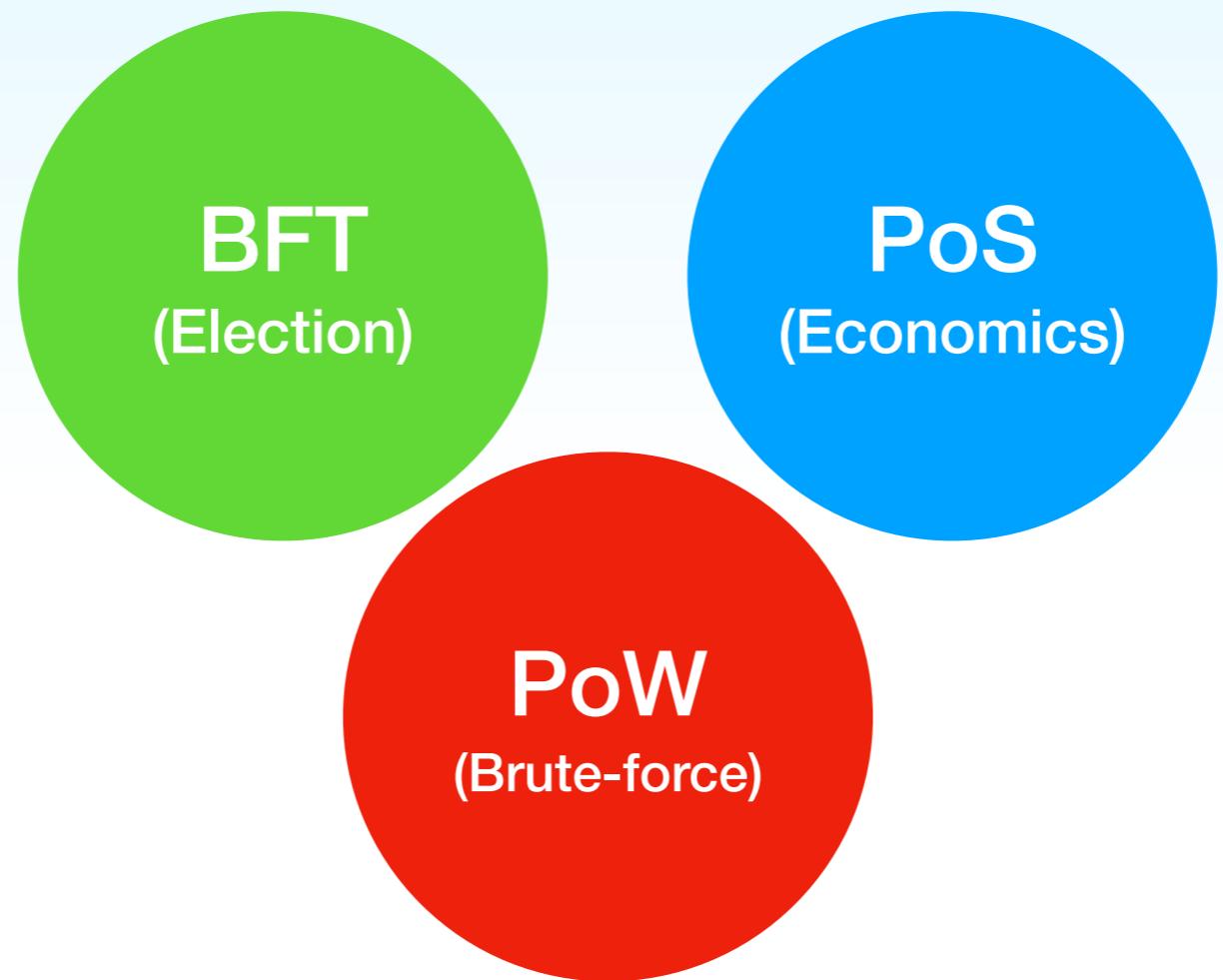
Synthesis Lectures on Data Management, Morgan & Claypool / Springer Publishers. 2019

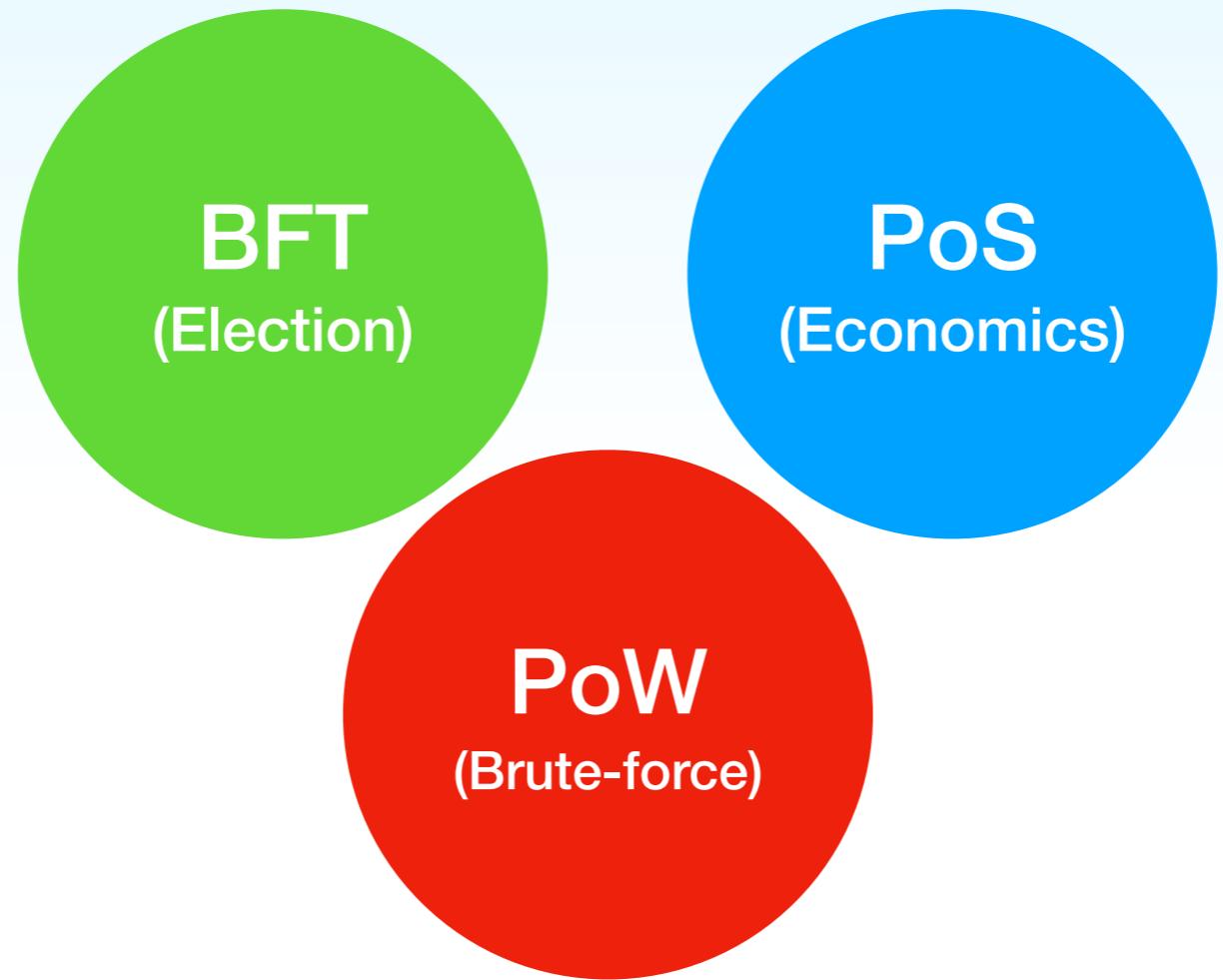
Chain Resiliency



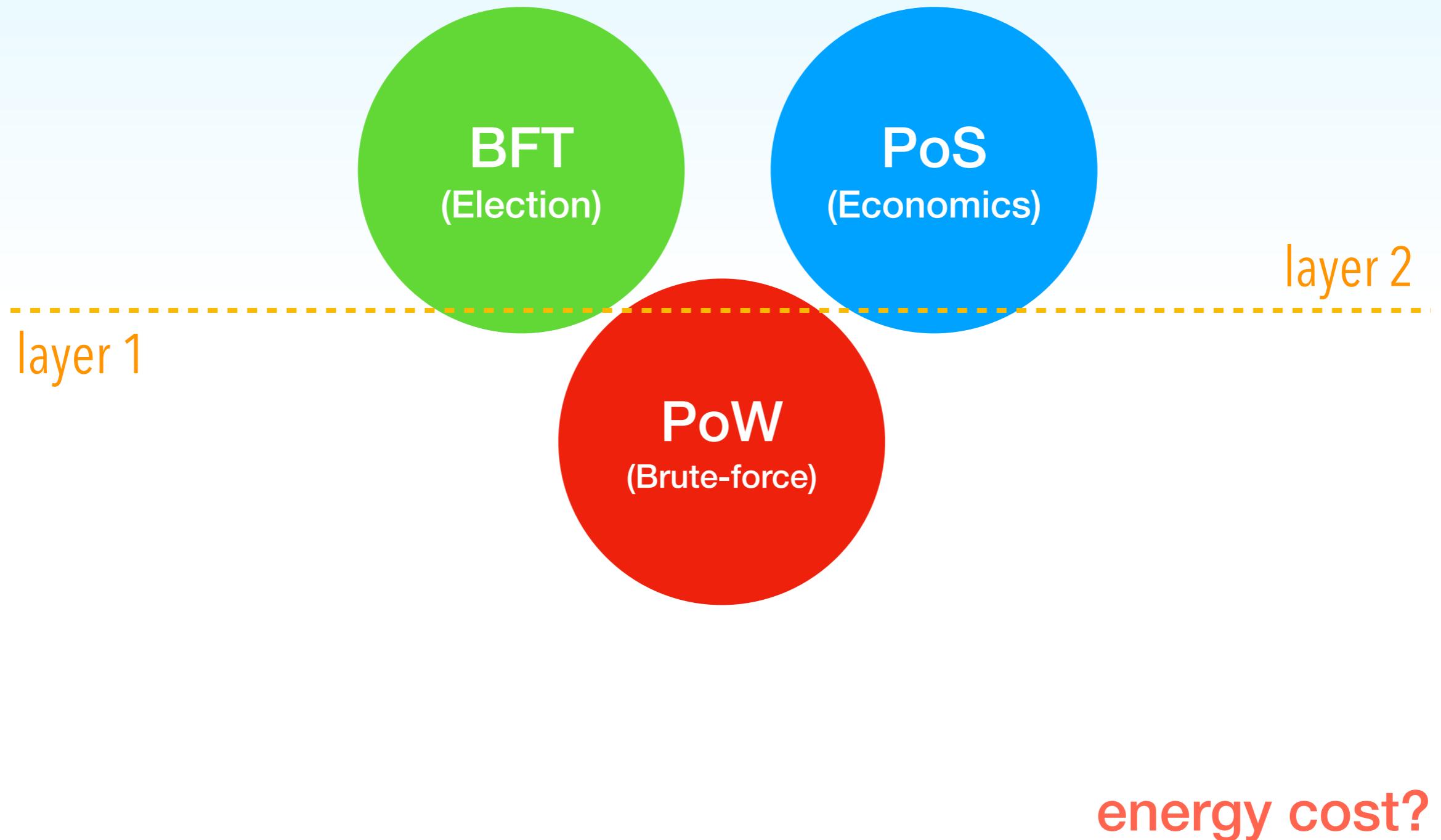
BFT
(Election)







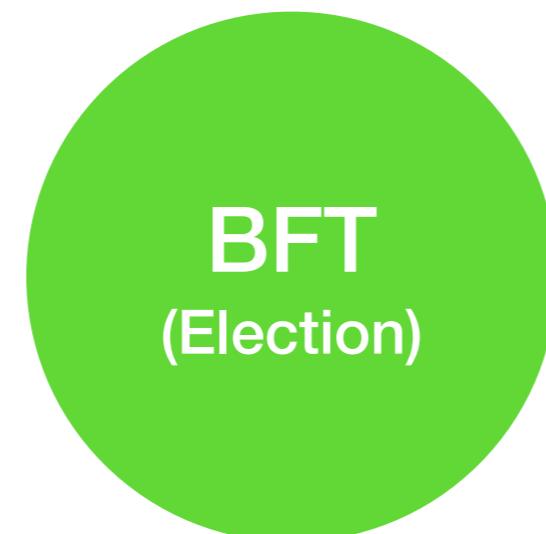
long-range attacks?



layer 2

collaboration vs. competition

layer 1

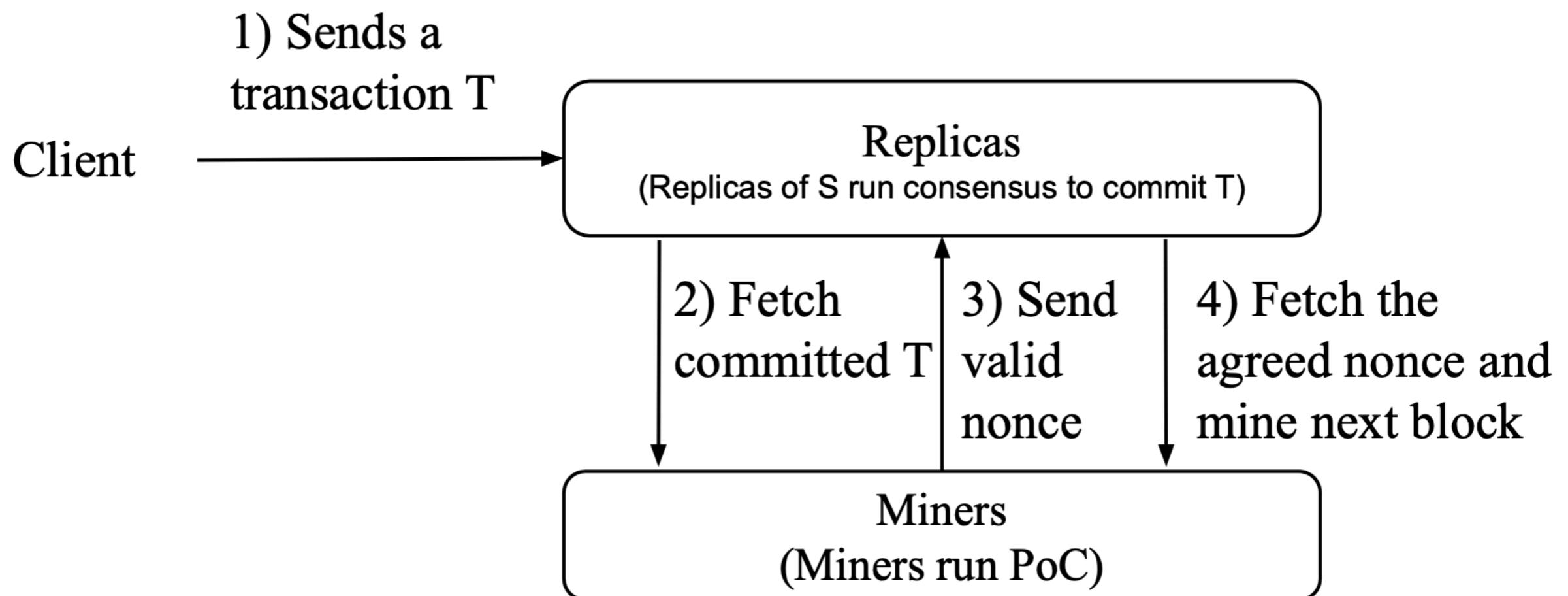






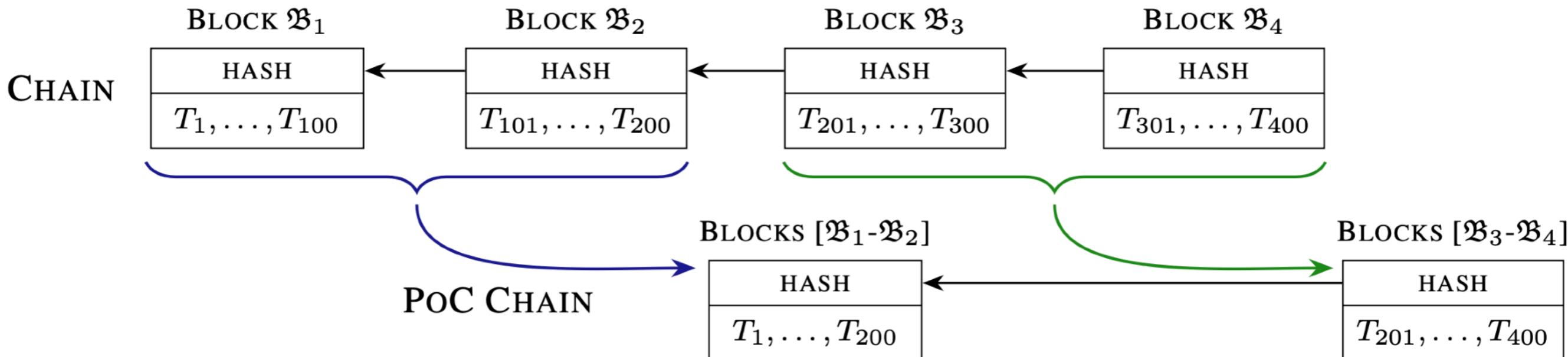
Hybrid Chain Application Flow

Every generated block is first finalized by consensus,
then notarized by collaborative mining.



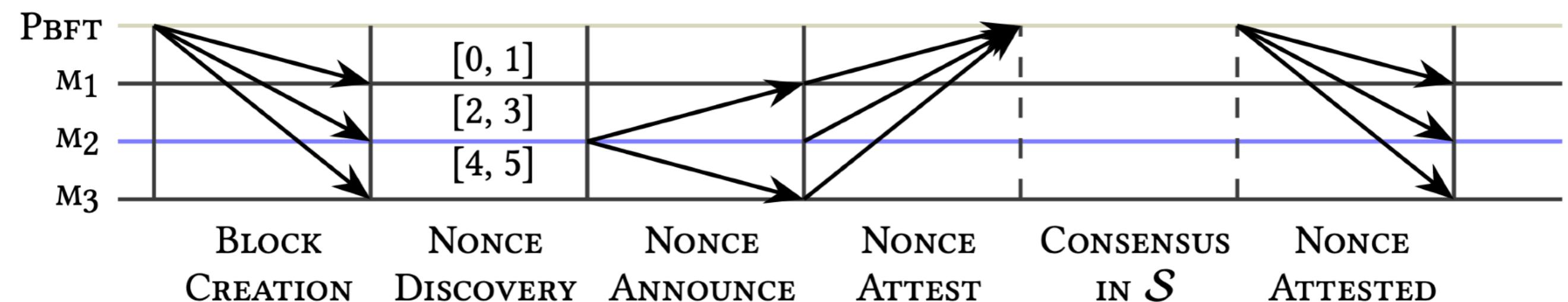
Hybrid Chain Architecture

Every agreed-upon block through consensus
has a dual block notarized by collaborative mining



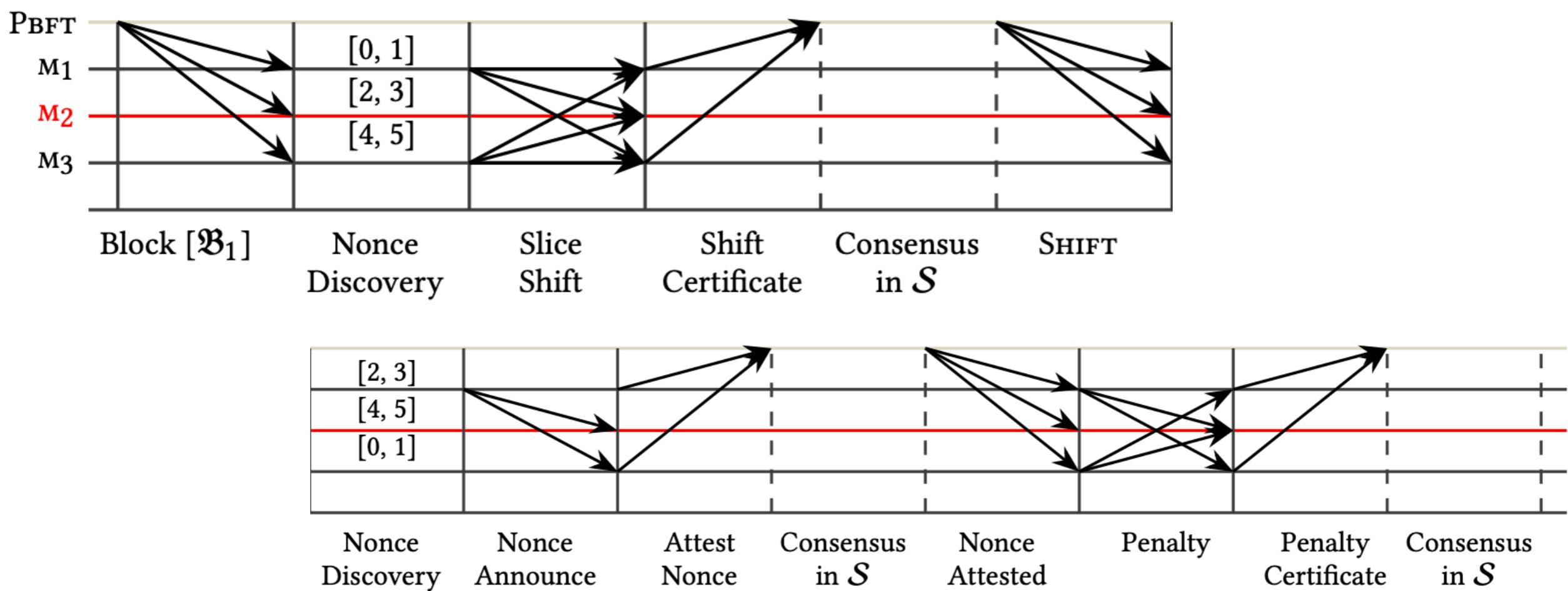
Hybrid Chain Protocol Flow

The consensus chain brings finality to transactions,
notary attestation, and reward.



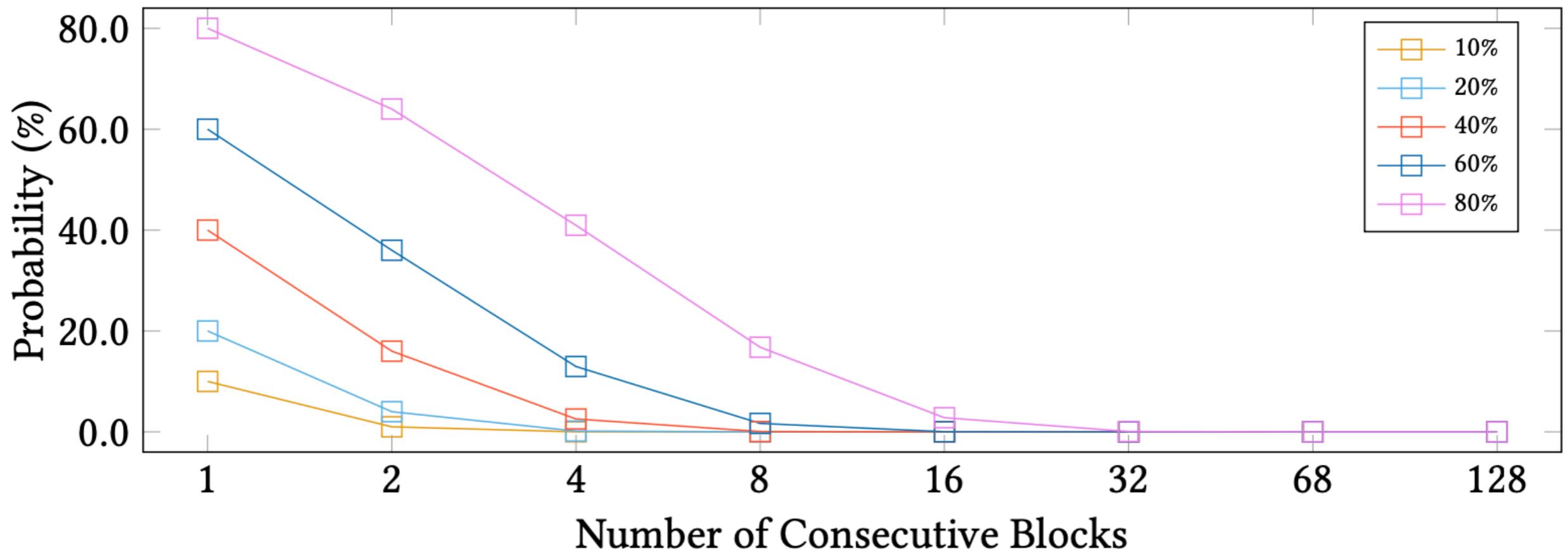
Hybrid Chain Recovery Flow

The consensus chain brings finality to mining failures and penalty attestation.



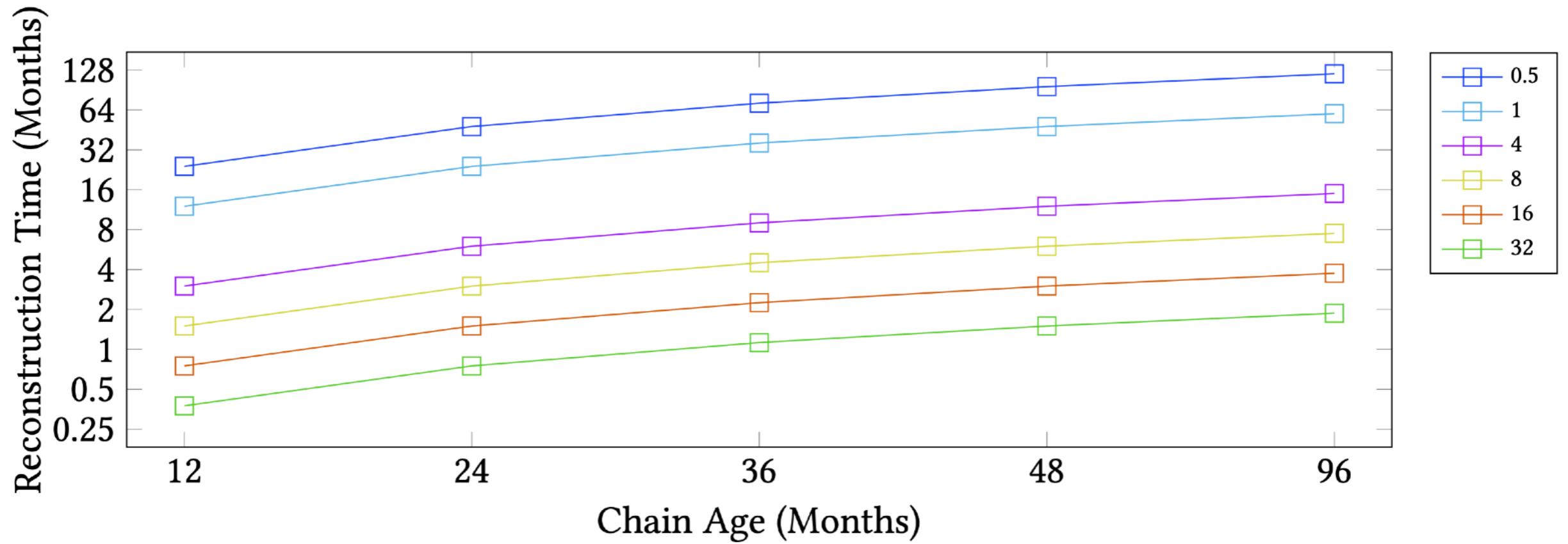
Long-Range Attacks Feasibility

In Power-of-Collaboration, the probability of successfully mining b-consecutive blocks decreases exponentially.



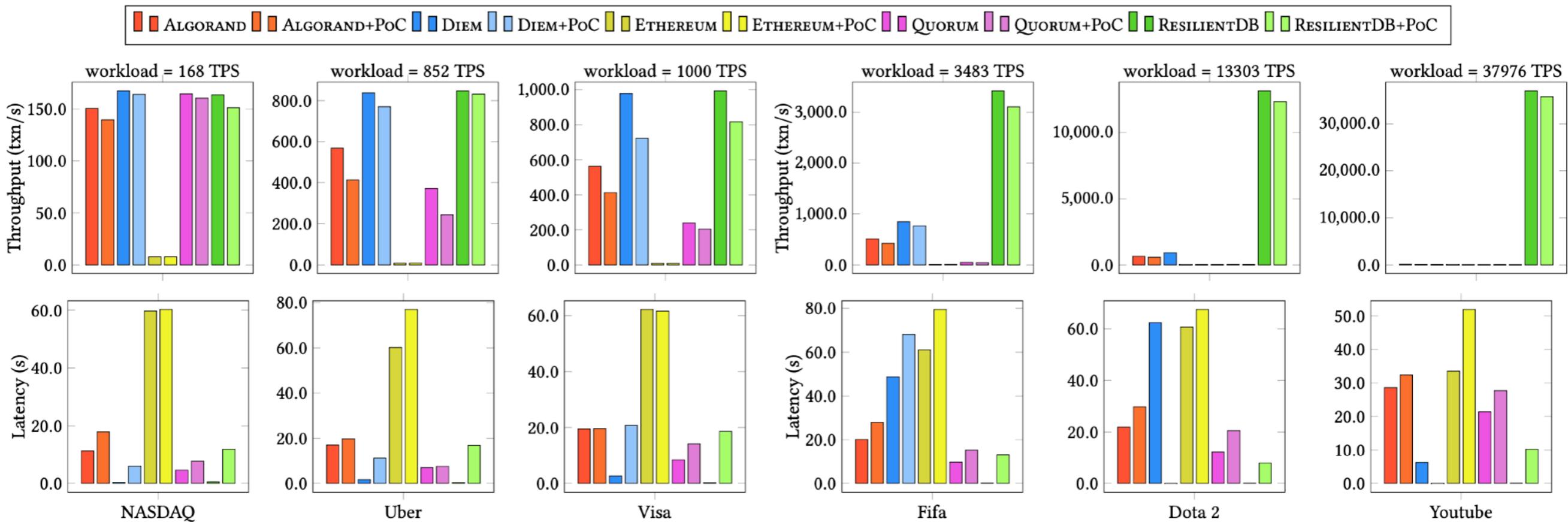
Long-Range Attacks Feasibility

In Power-of-Collaboration, rewriting history becomes prohibitively more expensive as the chain ages.



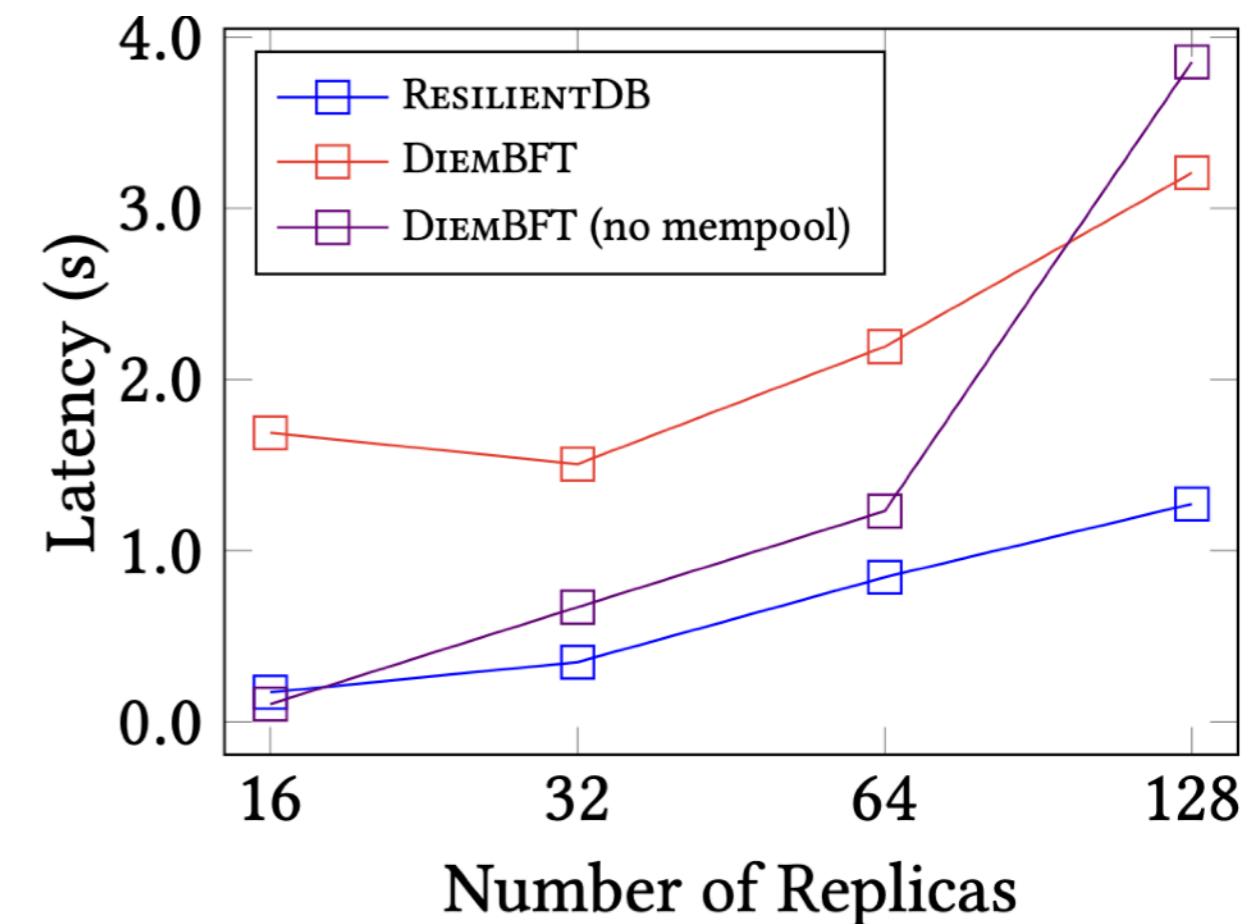
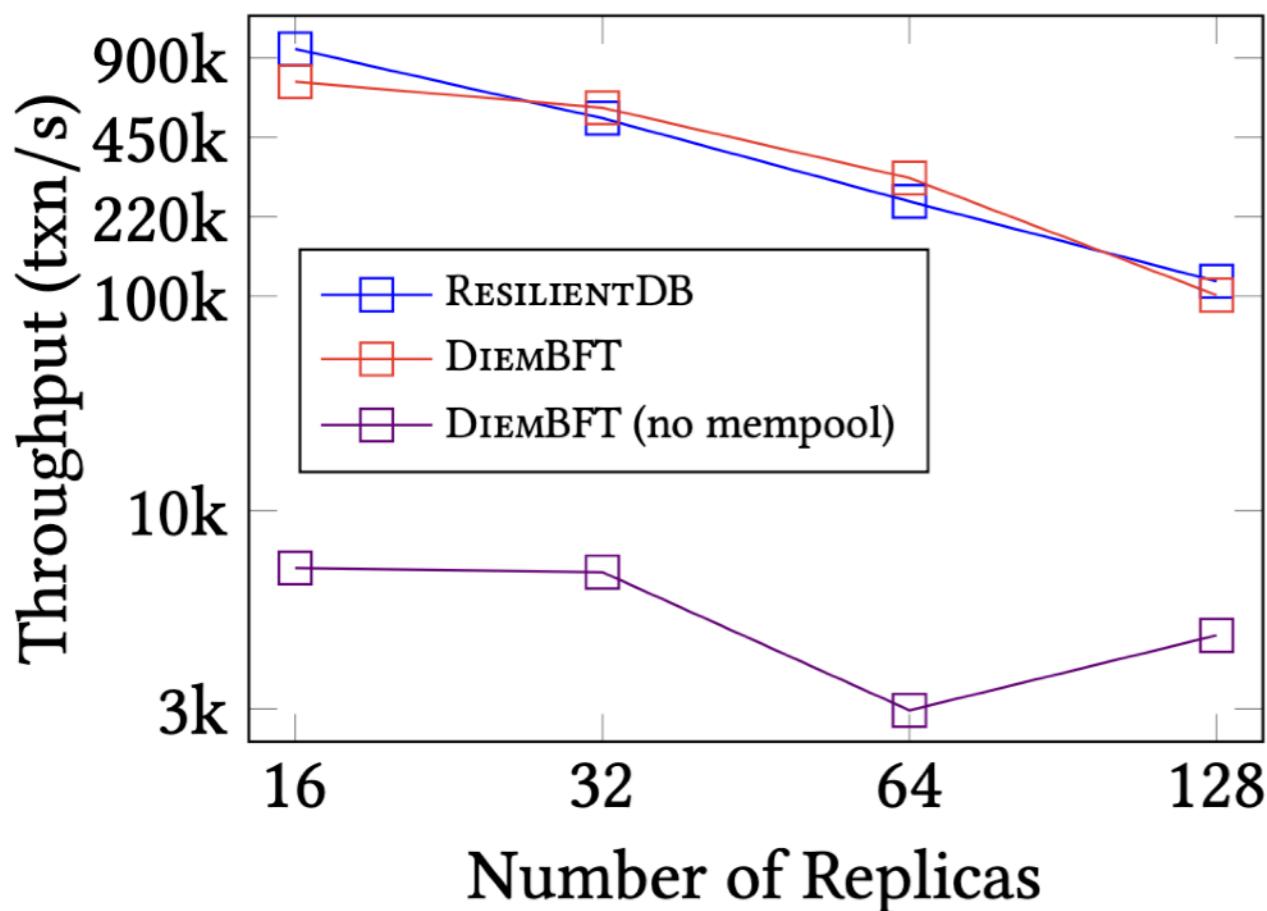
Power-of-Collaboration + System X

Collaborative mining as notary service results in negligible throughput and latency overheads.



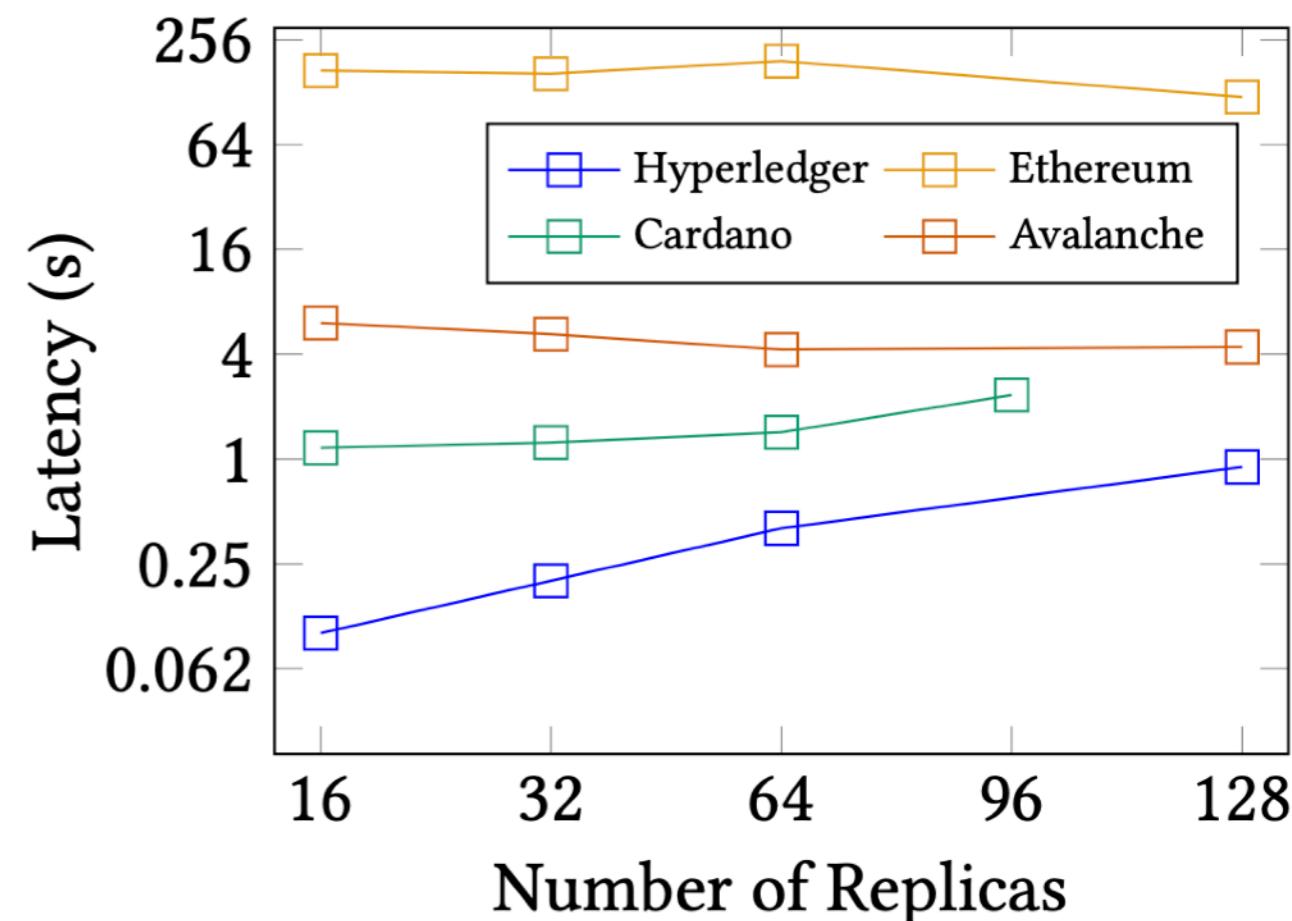
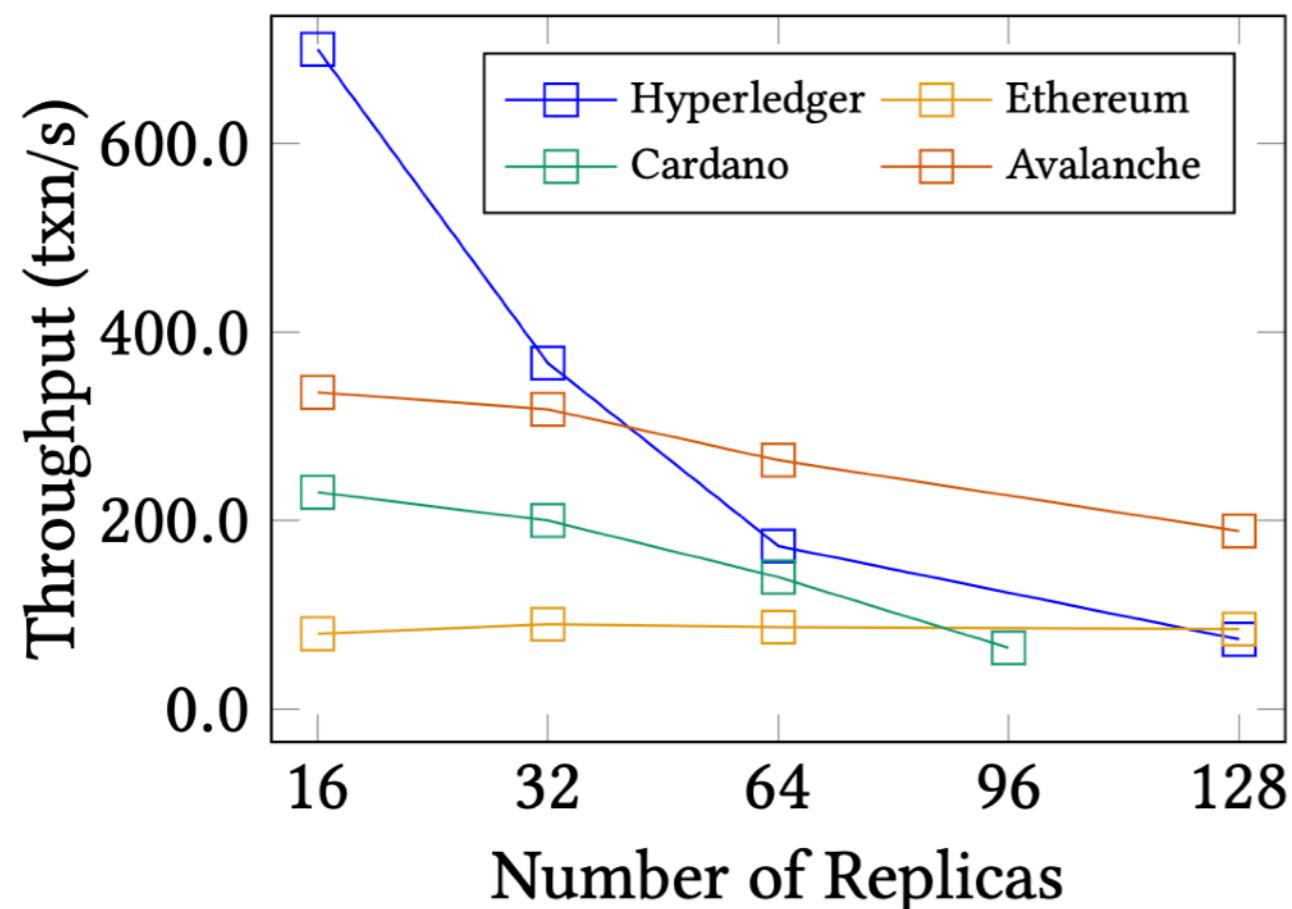
ResilientDB Performance

Highly optimized PBFT implementation in ResilientDB can sustain up to 900,000 transactions per seconds and scales up to hundreds of replicas.



ResilientDB Performance

Highly optimized PBFT implementation in ResilientDB + PoC can sustain up to 900,000 transactions per seconds and scales up to hundreds of replicas.



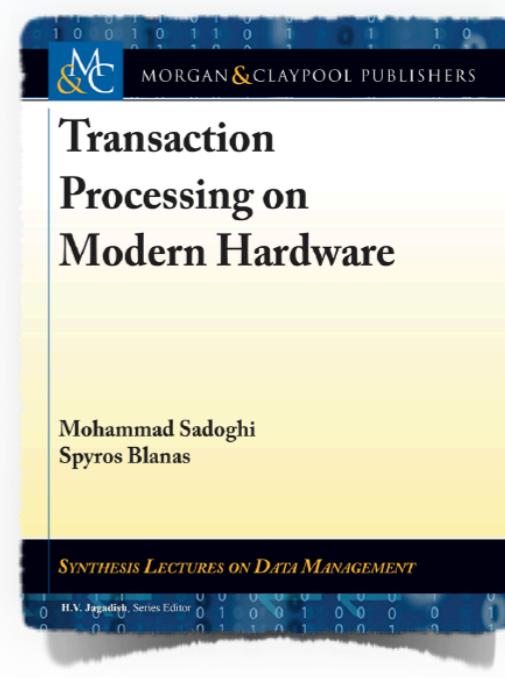
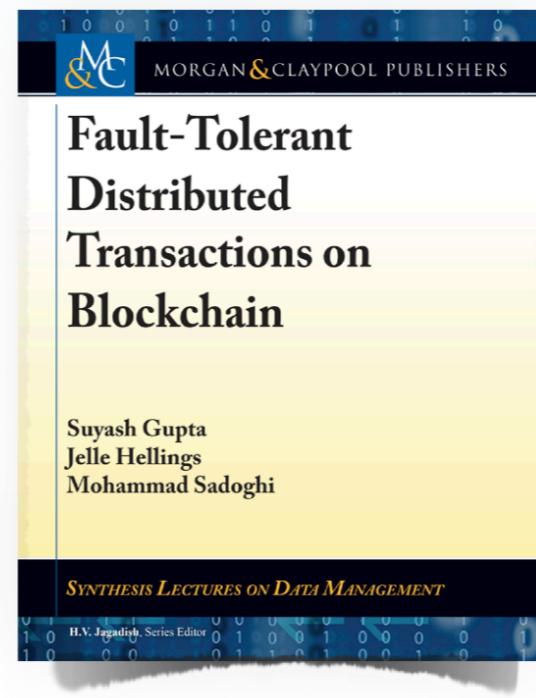
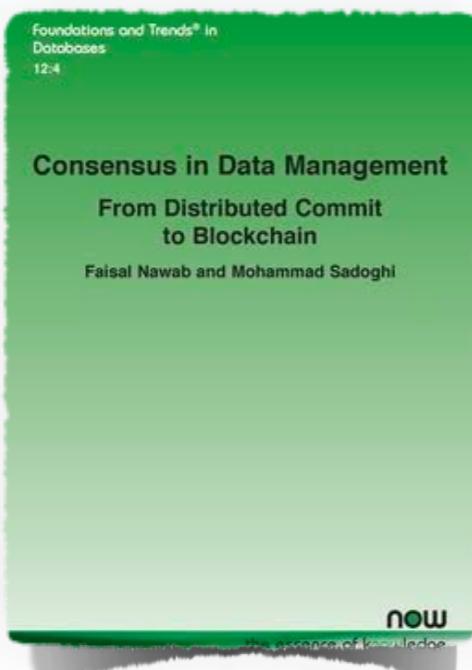
ResilientDB Performance

Transactions costs is orders of magnitude cheaper on ResilientDB

Blockchain	Cost Per 1000 Transactions
RESILIENTDB	\$0.00007
RESILIENTDB + PoC	\$0.000136
DIEMBFT	\$0.00019
HYPERLEDGER	\$0.08
AVALANCHE	\$0.155
CARDANO	\$0.239
ETHEREUM	\$14.66



THANK YOU



FOR COMPLETE REFERENCES

