Manifoldchain: Maximizing Blockchain Throughput via Bandwidth-Clustered Sharding

Chunjiang Che[1], Songze Li[2], Xuechao Wang[1]

1. The Hong Kong University of Science and Technology (Guangzhou)
2. Southeast University

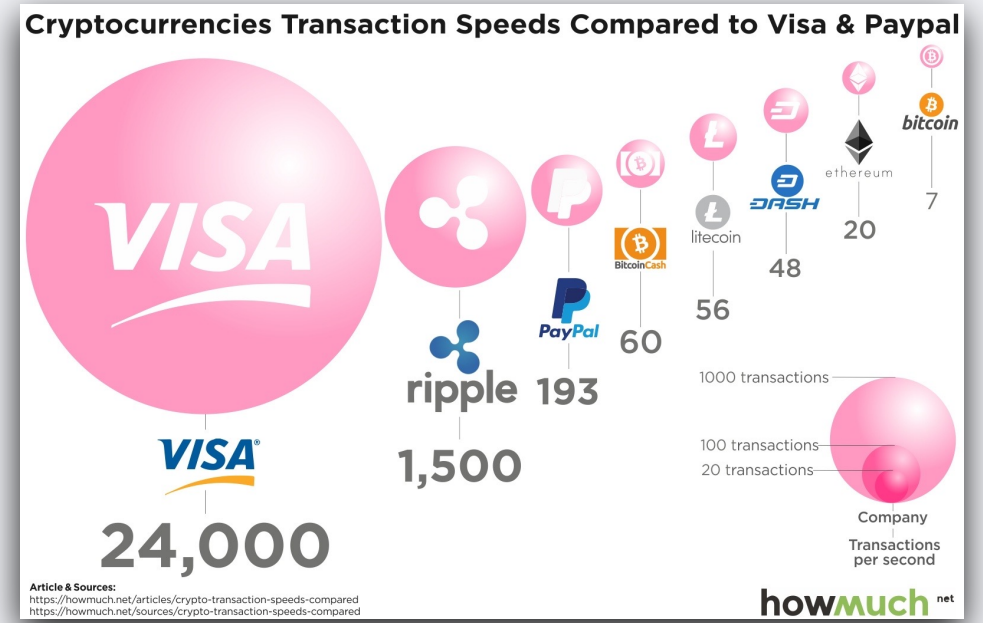
THE HONG KONG UNIVERSITY OF SCIENCE AND TECHNOLOGY (GUANGZHOU)

SOUTHEAST UNIVERSITY 東南大學 1902 南京

01

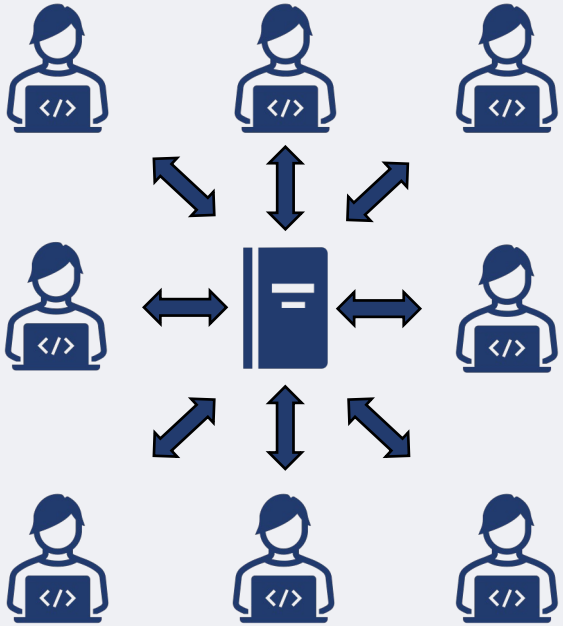
MOTIVATION

Blockchain Throughput



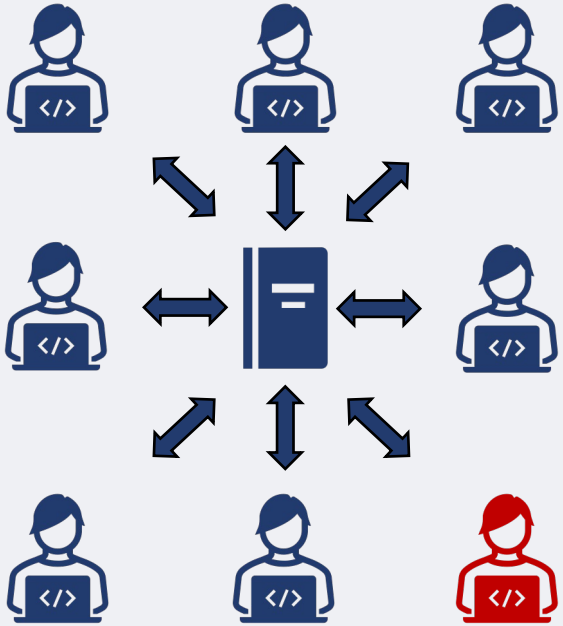
?

Bottleneck 1: Overlapping Tasks



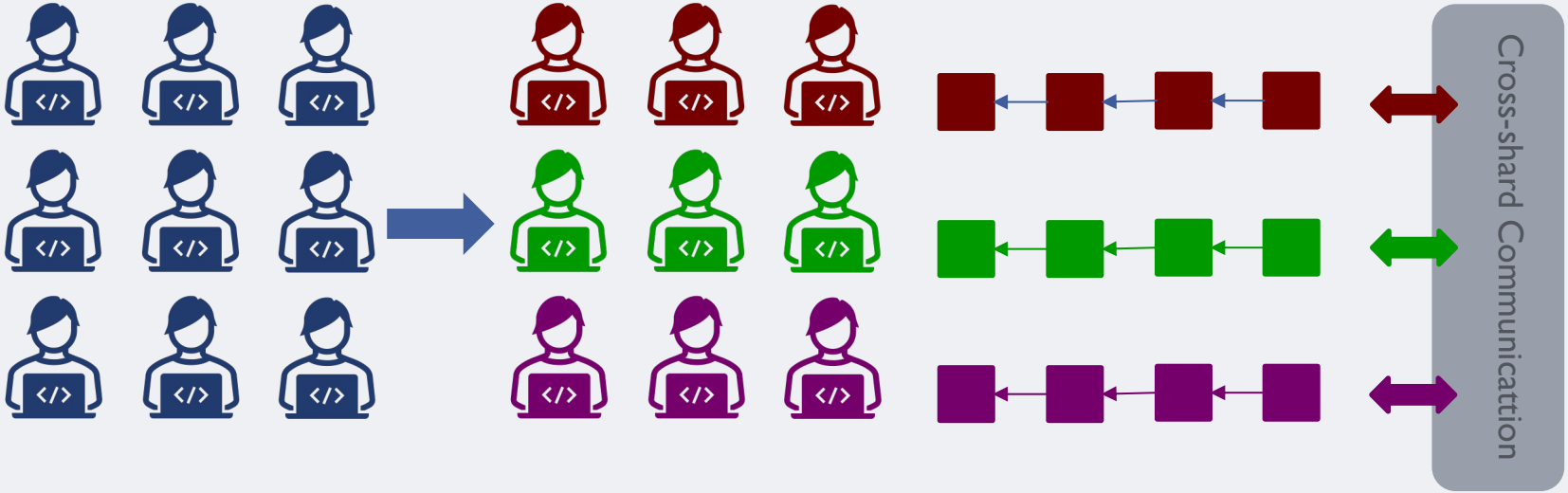
- Every miner replicates the entire ledger
- Highly overlapping computation, communication, and storage
- Throughput doesn't scale with the number of miners

Bottleneck 2: Stragglers



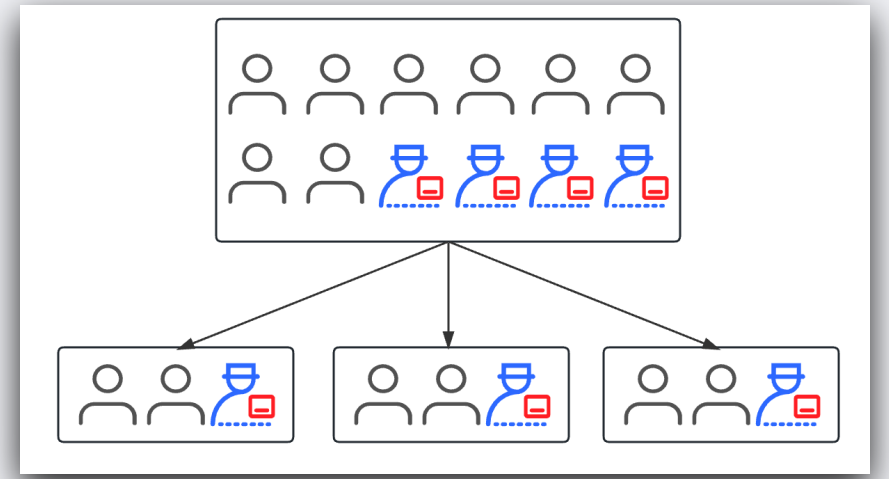
- Stragglers: limited bandwidth resources
- Fast miners need to wait for stragglers to synchronize the network.

Blockchain Sharding



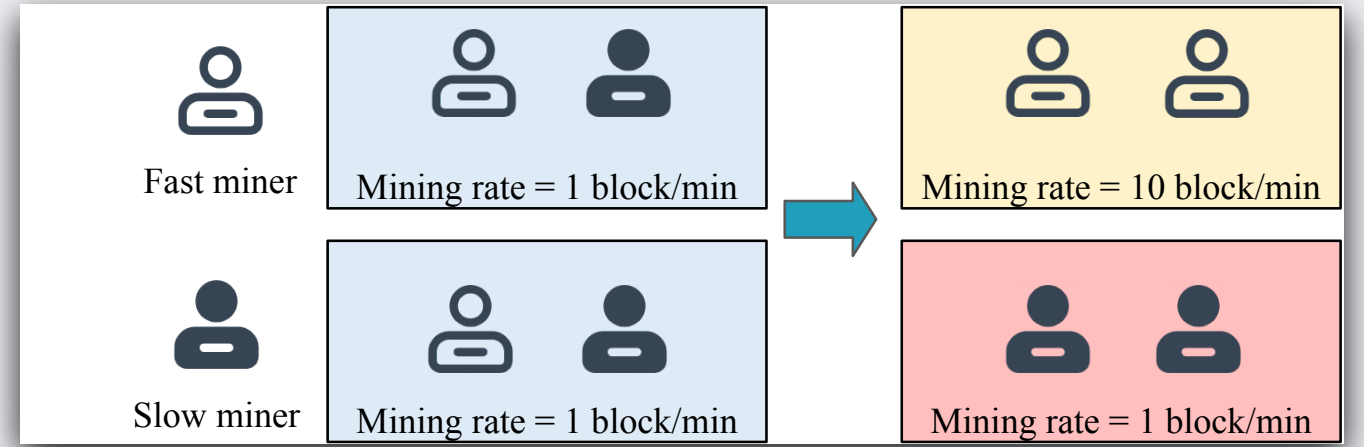
- Different shards maintain different ledgers
- Total throughput scales with the number of miners

SOTA Sharding Protocols Overlook Stragglers

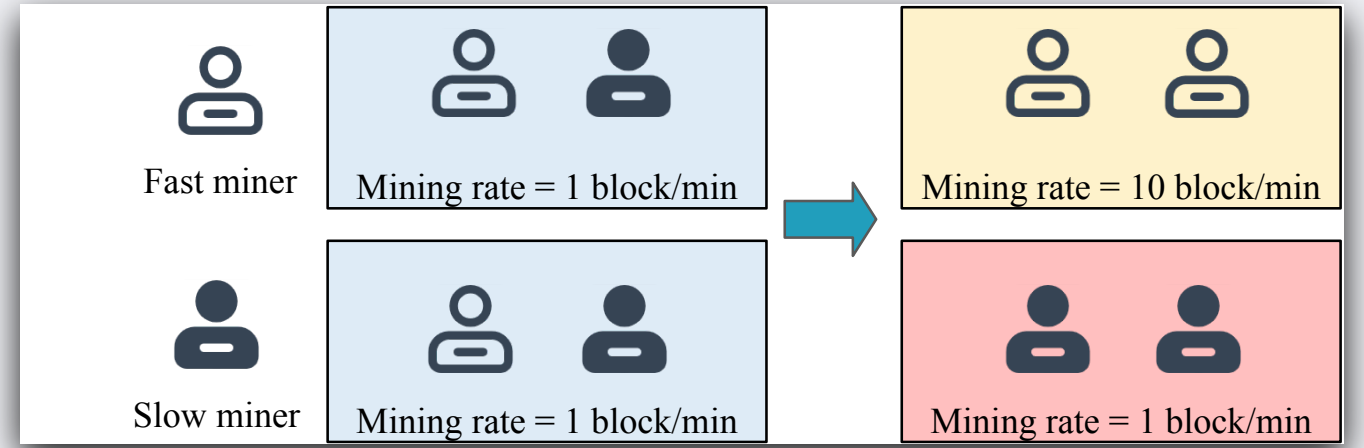


- Uniform shard formation (USF)
- Each shard contains stragglers

Bandwidth-Clustered Shard Formation (BCSF)

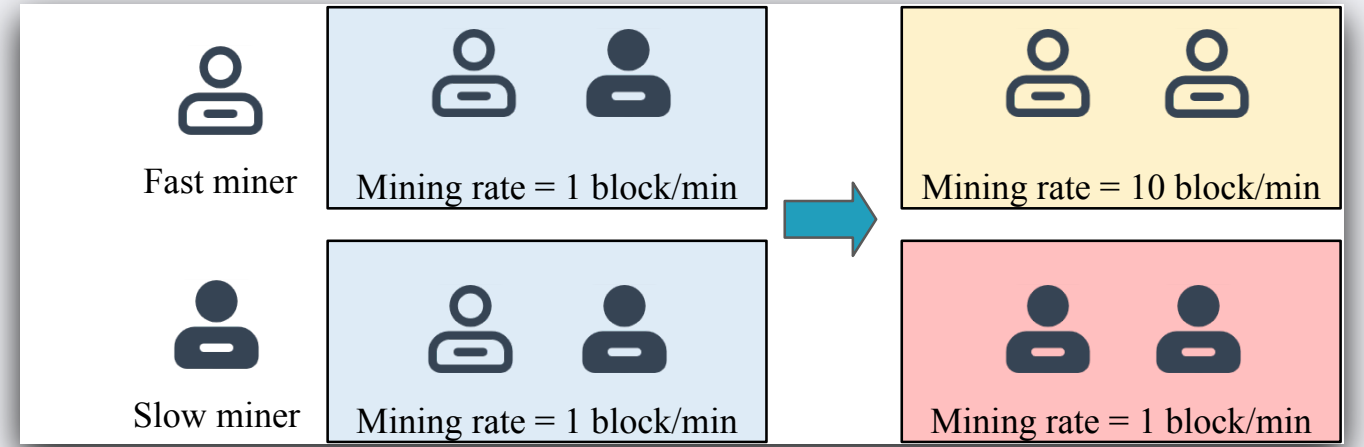


Bandwidth-Clustered Shard Formation (BCSF)



Naive?

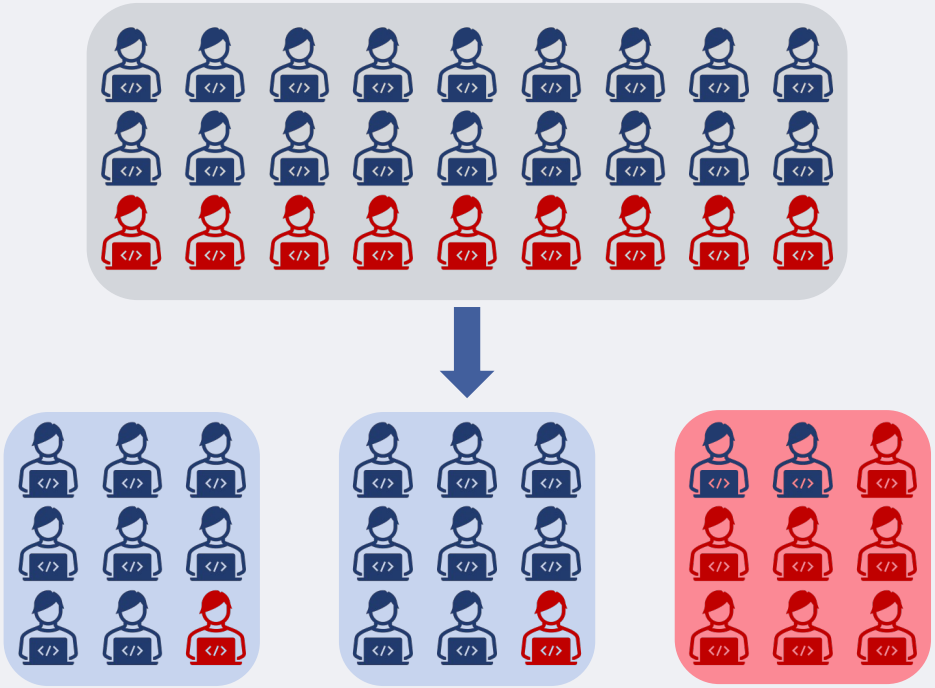
Bandwidth-Clustered Shard Formation (BCSF)



Naive?

Hard to achieve!

New Challenge: Adversarial Concentration



- Corrupted miners pretend to have closed bandwidths
- Adversarial ratio >= 50%
- No consensus protocol works under adversarial majority!

High-level Insight

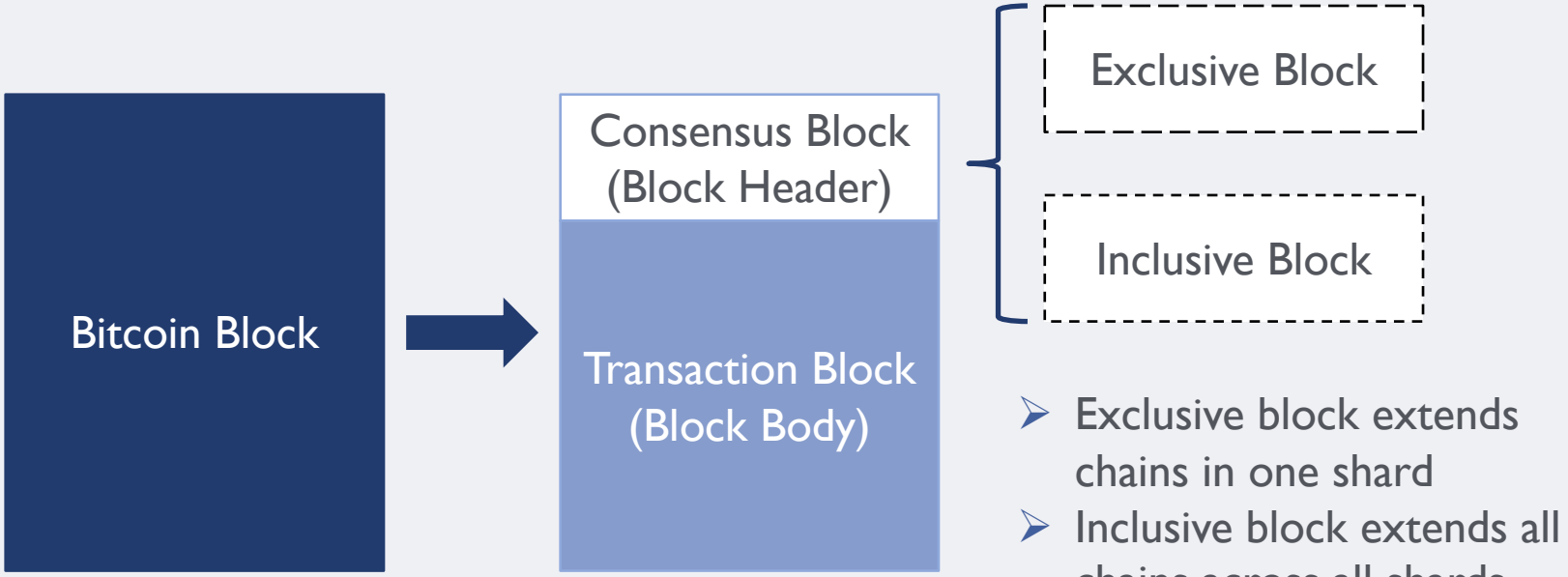
We propose **sharing mining** to ensure security as long as each shard has one honest miner

- Honest miners share blocks across shards to diffuse their hashing power to other shards

02

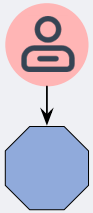
METHOD

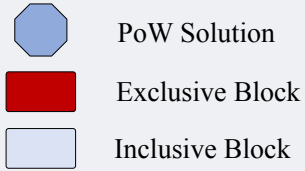
Block Structure



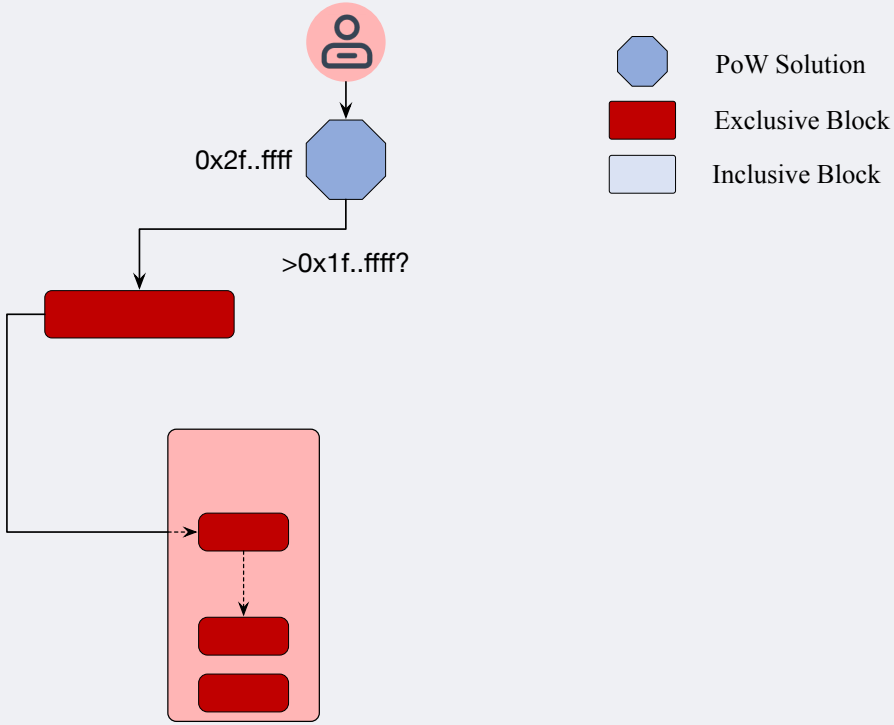
- Exclusive block extends chains in one shard
- Inclusive block extends all chains across all shards

Sharing Mining

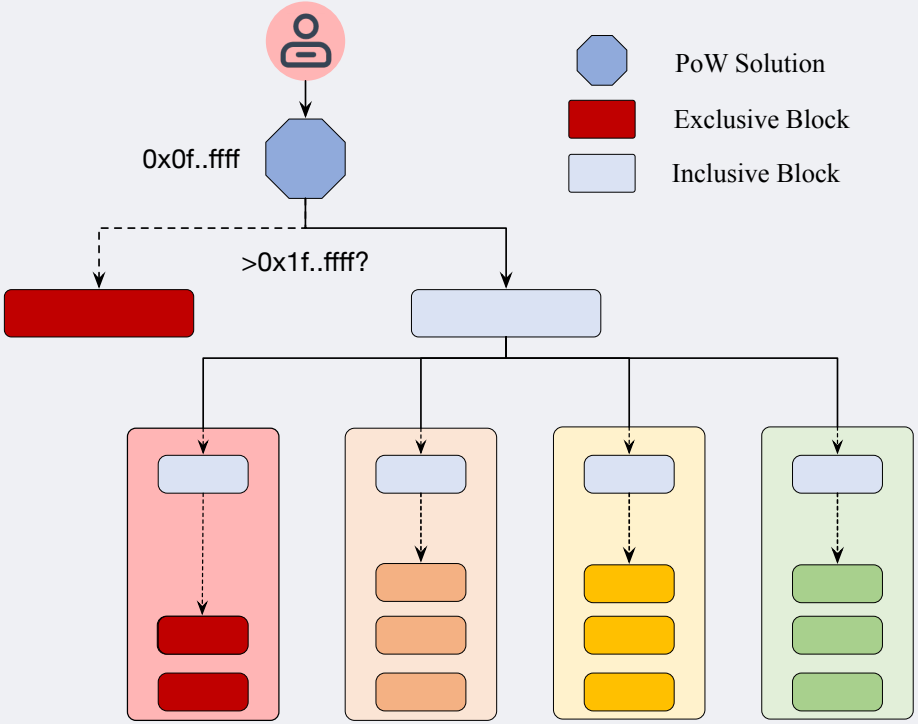


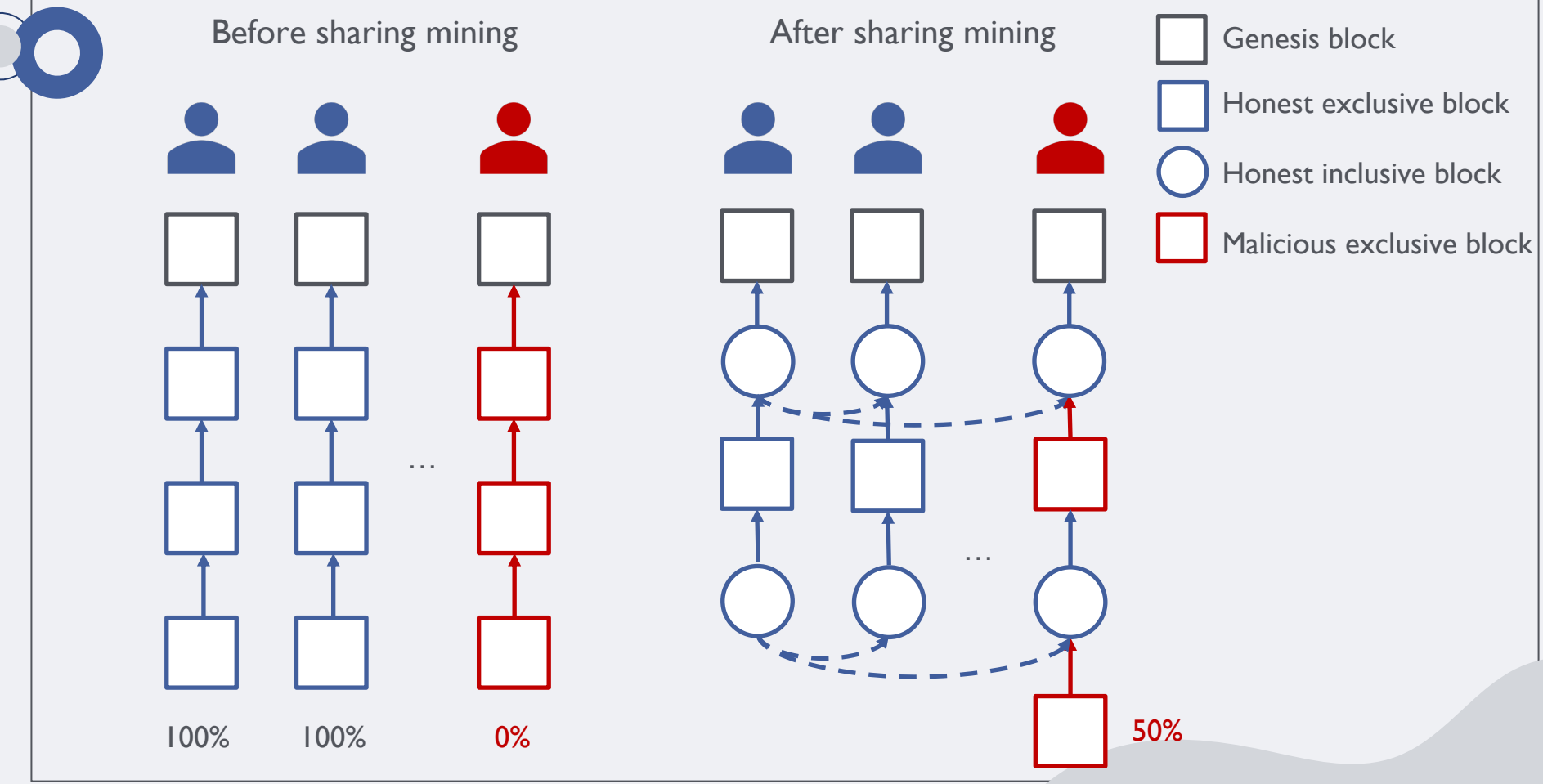


Sharing Mining

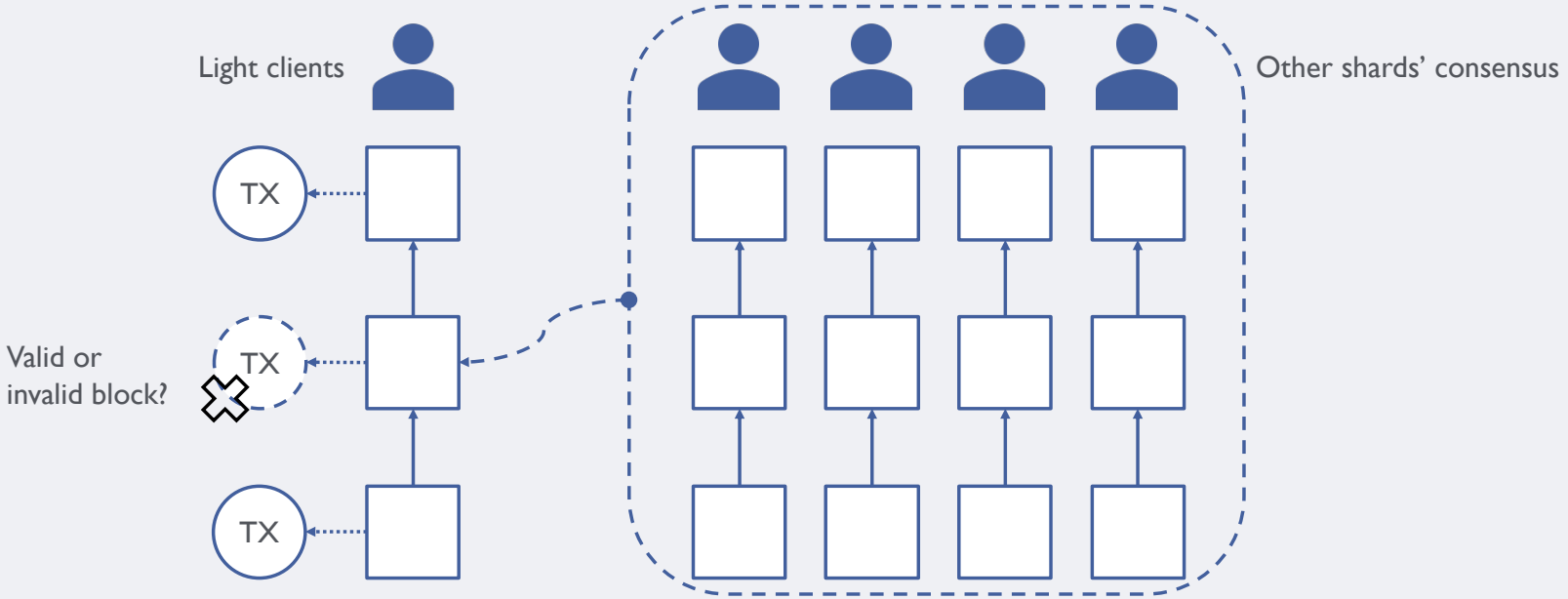


Sharing Mining

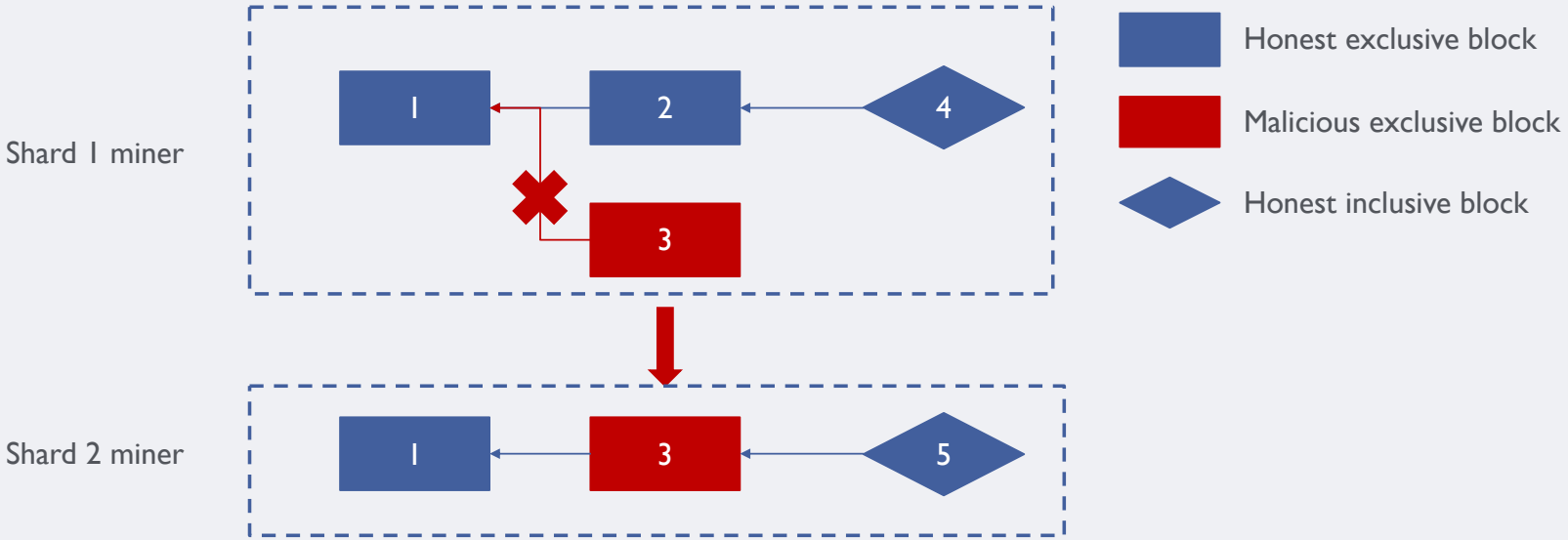



Before sharing mining
After sharing mining
Genesis block
Honest exclusive block
Honest inclusive block
Malicious exclusive block
100%
100%
0%
50%

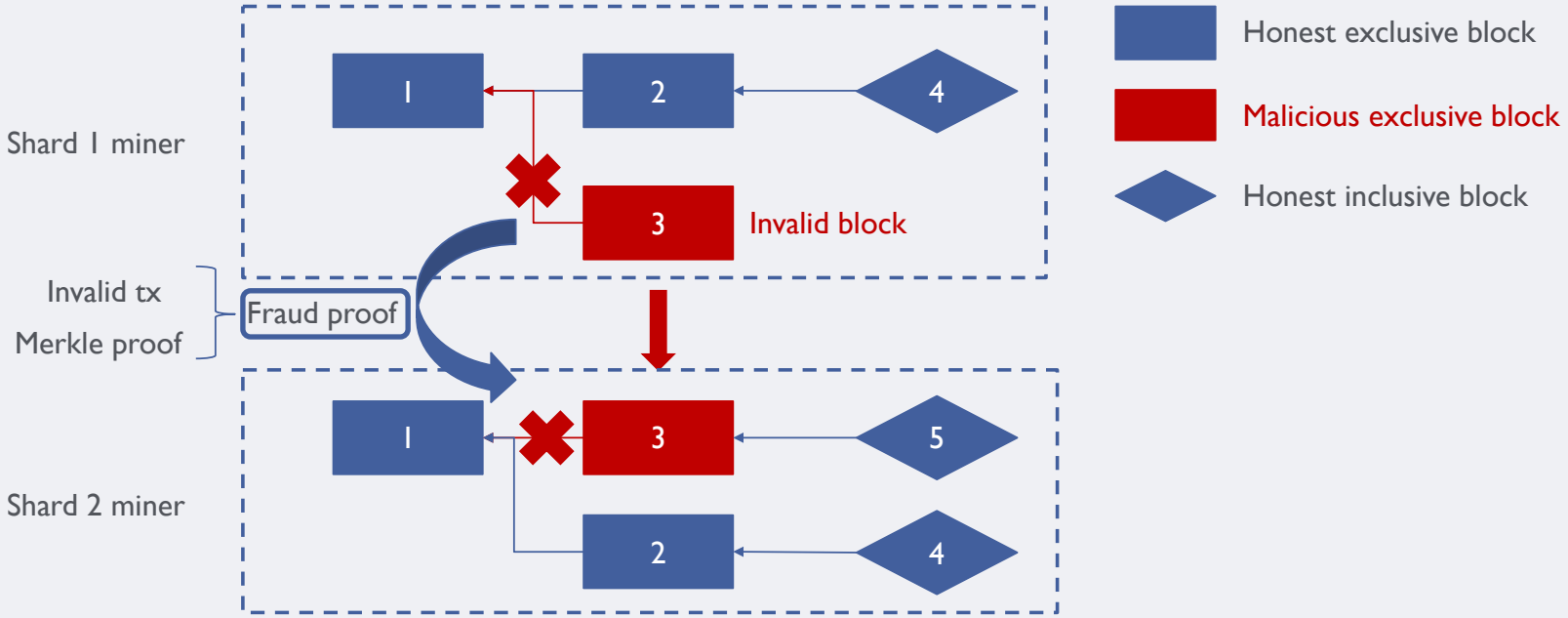
Light Client (SPV)



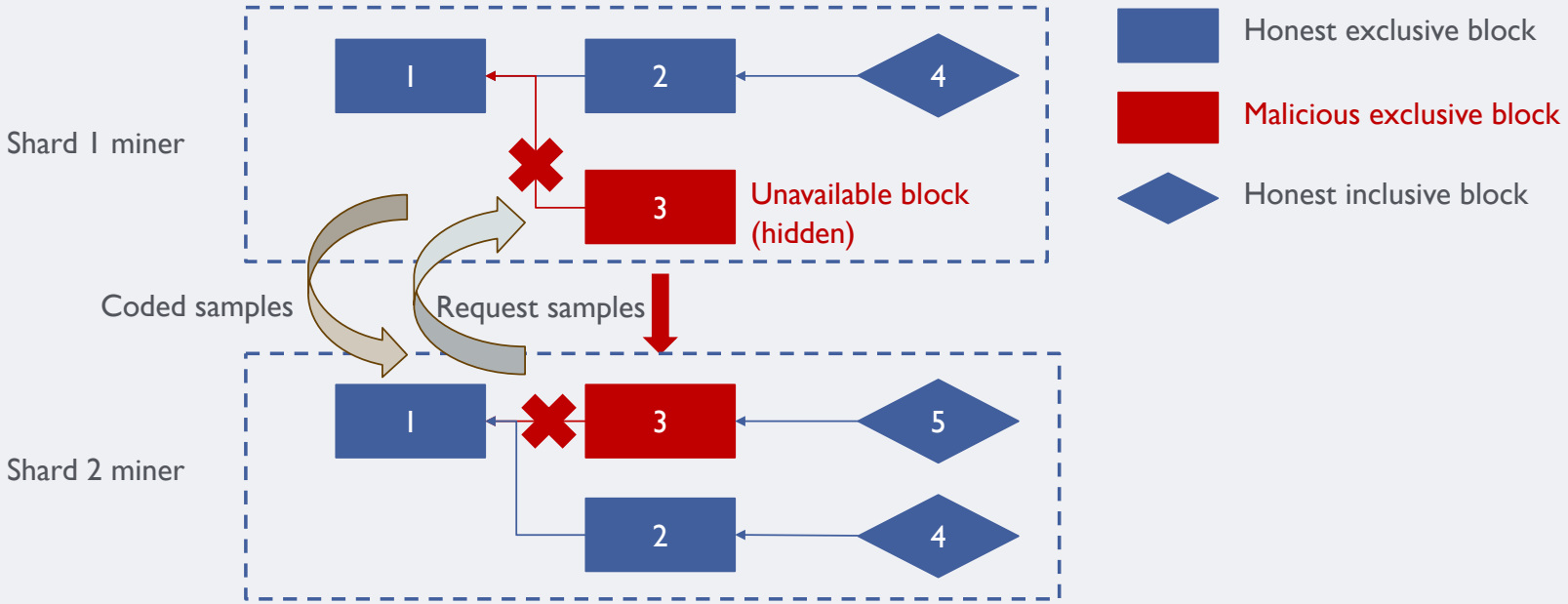
Hashing Power Splitting Attack



Transaction Validity Verification

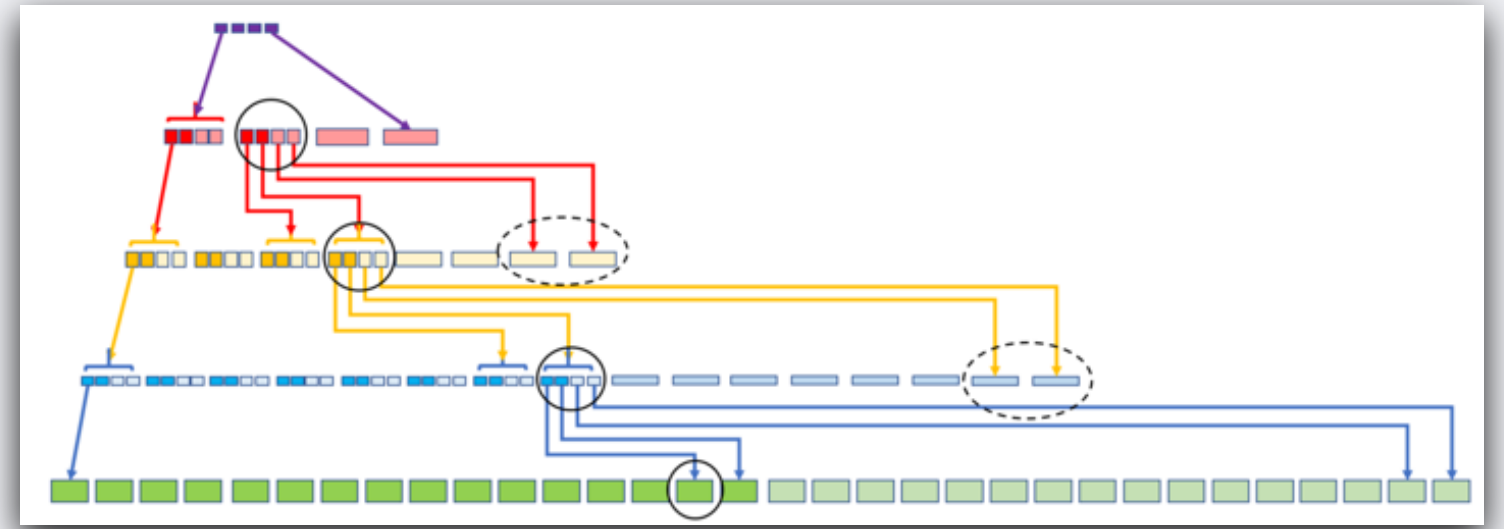


Data Availability Verification



Coded Merkle Tree

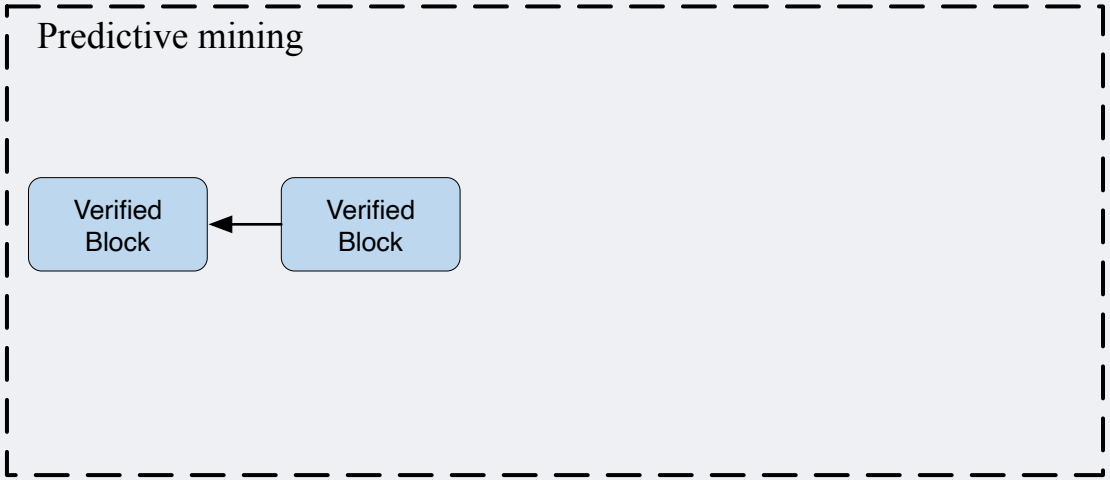
[1]



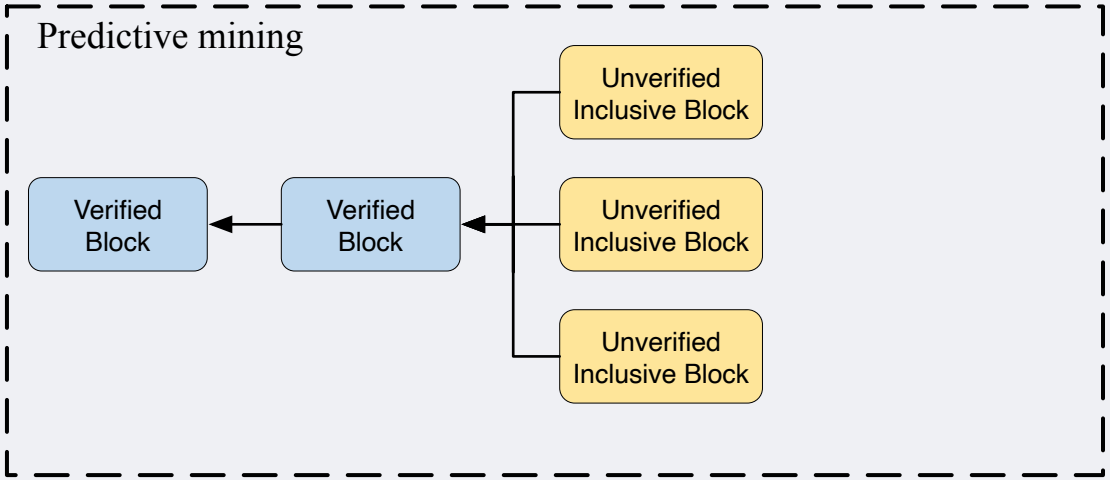
Miners only need to sample $O(\log B)$ bytes

[1] Yu, M., Sahraei, S., Li, S., Avestimehr, S., Kannan, S., & Viswanath, P. (2020, February). Coded merkle tree: Solving data availability attacks in blockchains. In International Conference on Financial Cryptography and Data Security (pp. 114-134). Cham: Springer International Publishing.

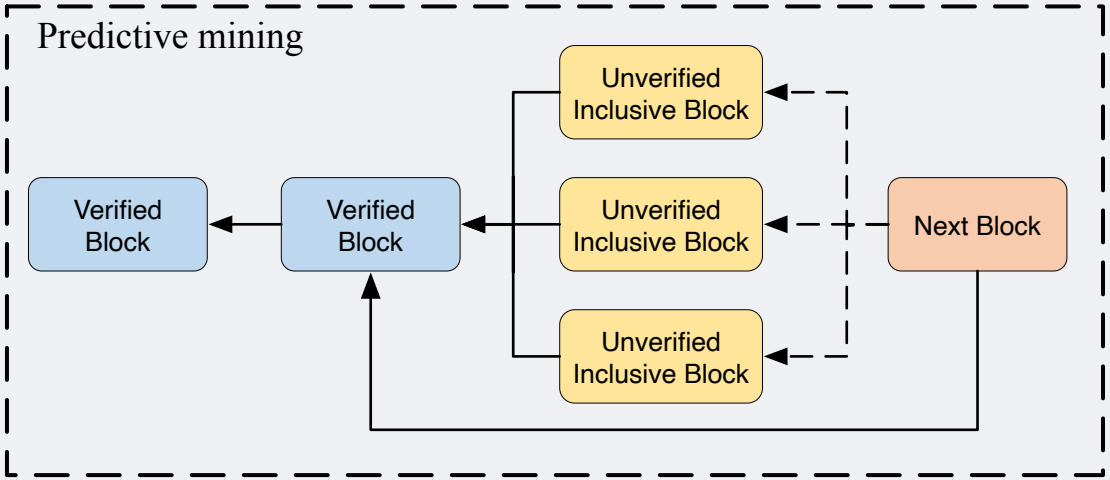
Predictive Mining



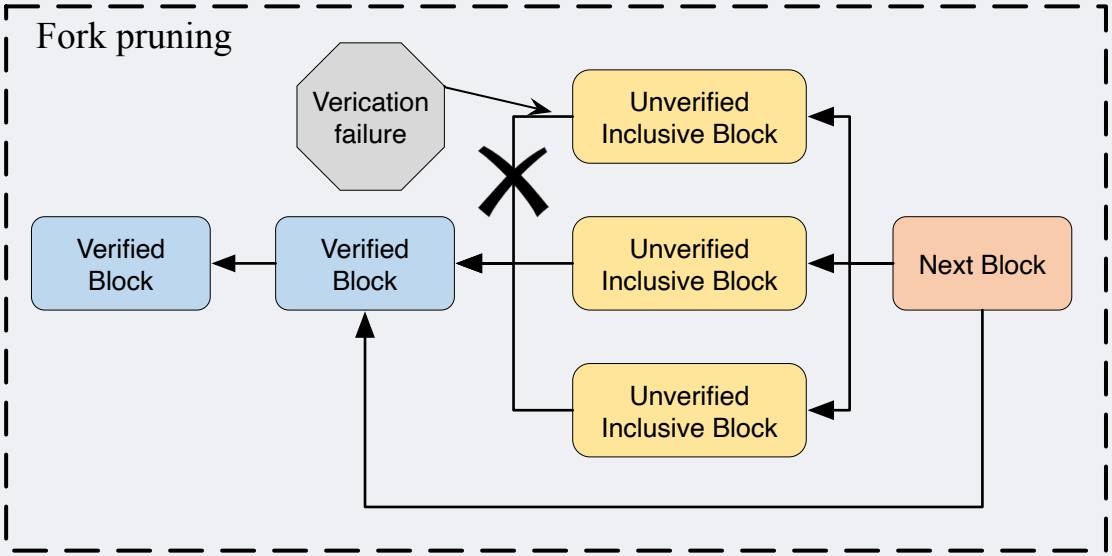
Predictive Mining



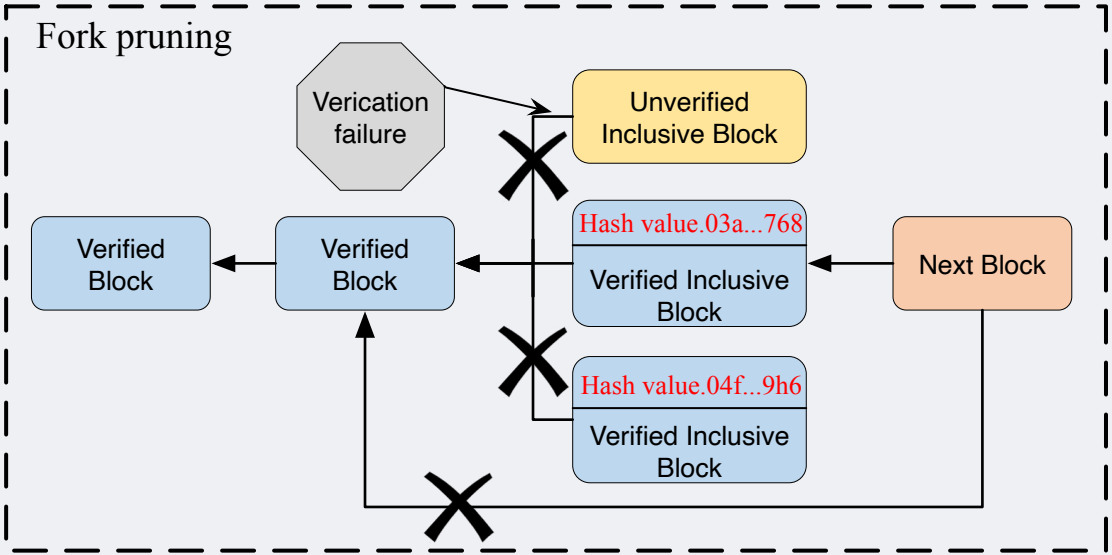
Predictive Mining



Fork Pruning



Fork Pruning



03

Theoretical Analysis

Security Analysis

Theorem 1 (informal)

If there is one honest miner in each shard, Manifoldchain holds Common Prefix, Chain Growth, and Chain Quality within each shard, regardless of the adversary's attack strategy, as long as $\rho \geq 1/2$ except with a negligible probability.

Manifoldchain is secure as long as the majority of miners are honest.

Throughput Analysis

Theorem 2 (informal)

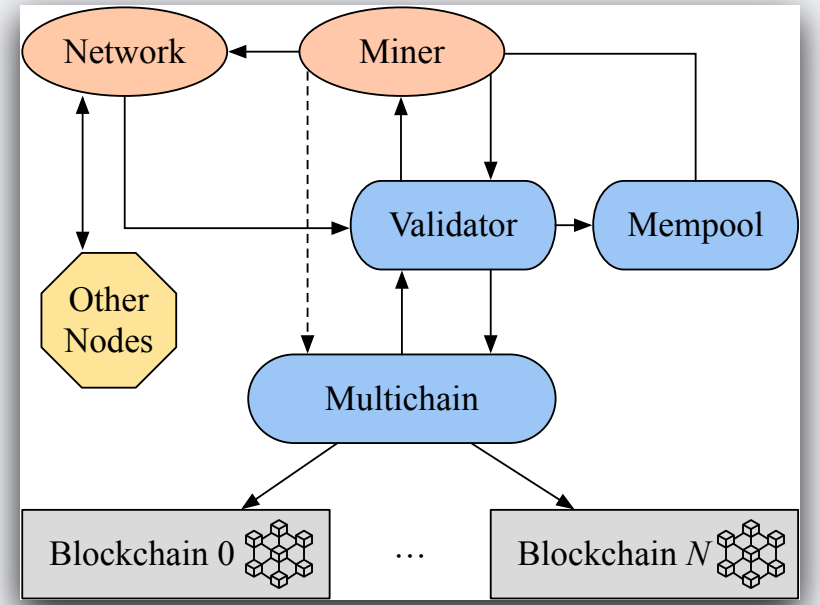
In a scenario where Bitcoin achieves a throughput of T, Manifoldchain attains a throughput of $\sum_i^m T \frac{\Delta}{\Delta_i} \frac{\rho_i}{\rho}$, while maintaining the same level of security as Bitcoin.

The total throughput is scalable with bandwidth (in fast shards where $\Delta_i < \Delta$, throughput scale from T to $\frac{\Delta}{\Delta_i} T$), and at worst case (where $\Delta_i = \Delta$), Manifoldchain achieves the same throughput as Bitcoin within each shard.

04

Evaluation

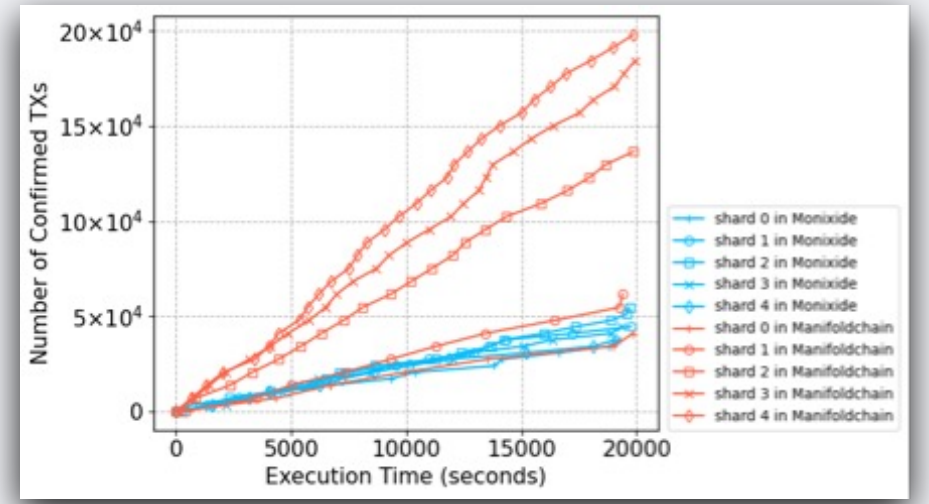
Implementation

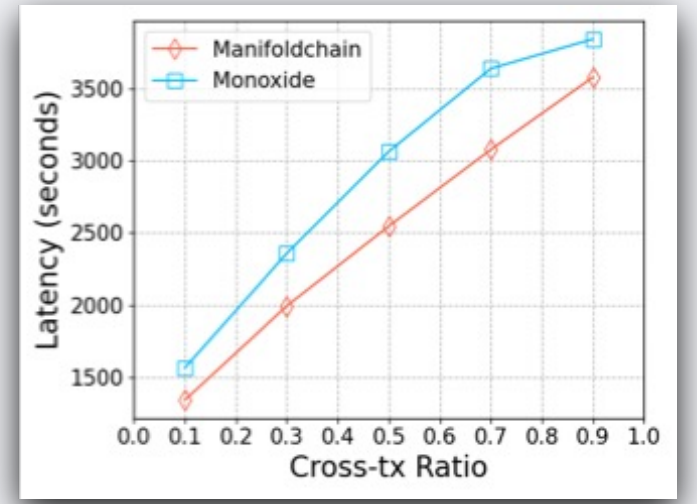


- A complete prototype (over 15,000 lines of Rust code)
- With higher throughput than the SOTA sharding protocol (under same testbed)
- Evaluated on real-world scenario (AWS EC2)

Scalability on Amazon EC2

- Bandwidth configuration: {5, 10, 20, 40, 60} x 10
- Shard formation: Monoxide adopts USF, Manifoldchain adopts BCSF





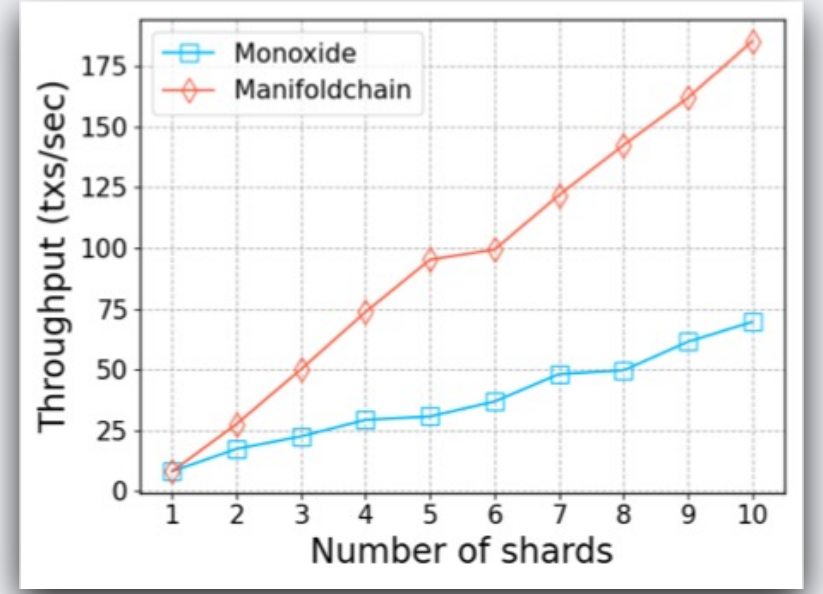
Higher throughput, lower latency

Horizontal Scalability

With each increment in m, add 5 miners with the bandwidth of {5, 10, 20, 40, 60} Mbps

- Manifoldchain: 20 tx/sec for each increment
- Monoxide: 7 tx/sec for each increment

As the number of miners increases, Manifoldchain achieves greater throughput increments.

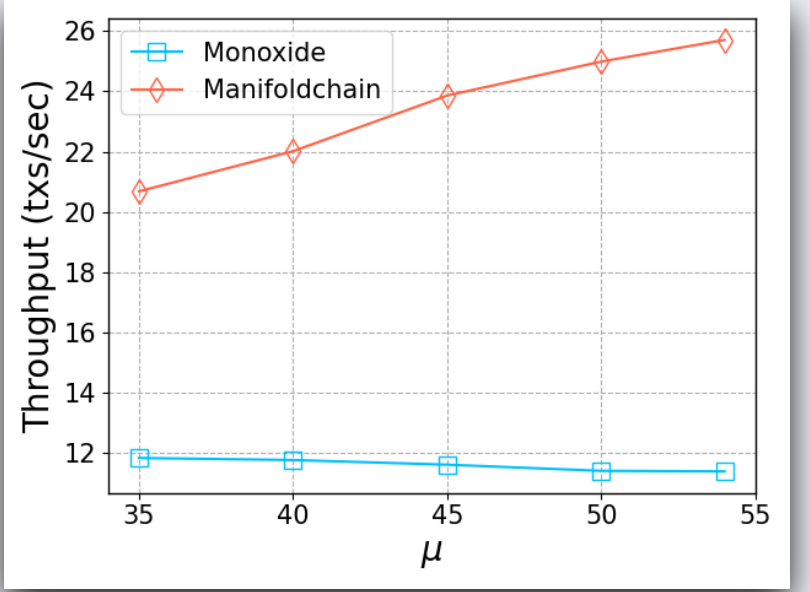


Vertical Scalability

20 normal miners and 5 stragglers

- Stragglers follow $\mathcal{N}(10, 2)$
- Normal miners follow $\mathcal{N}(\mu, 7)$
- Manifoldchain: 1.25tx/sec for each increment
- Monoxide: constant

With same bandwidth resources, Manifoldchain achieves higher throughput.



THANKS

Do you have any questions?

cche861@connect.hkust-gz.edu.cn