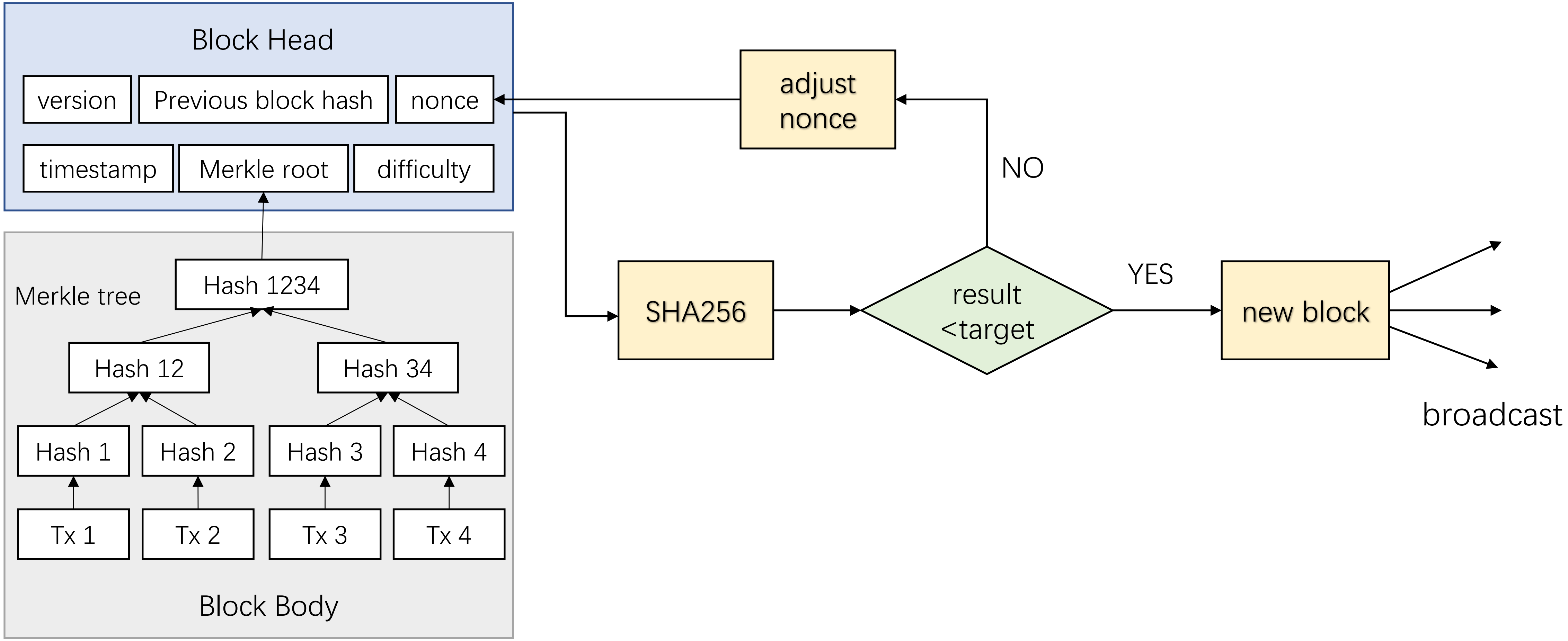
Monoxide: Scale out Blockchains with Asynchronous Consensus Zones

Jiaping Wang, Hao Wang

USENIX NSDI 2019

Background

➢Block Structure & Proof-of-Work (PoW)



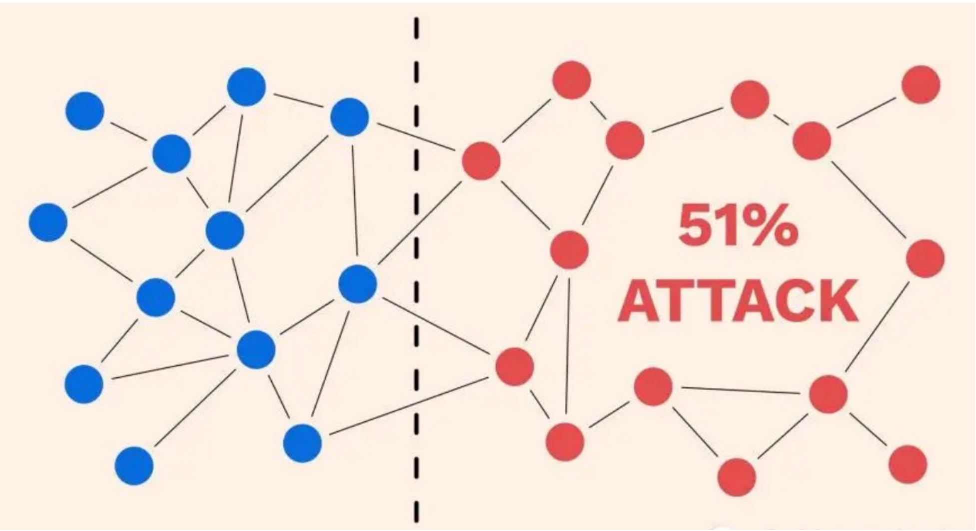
Background

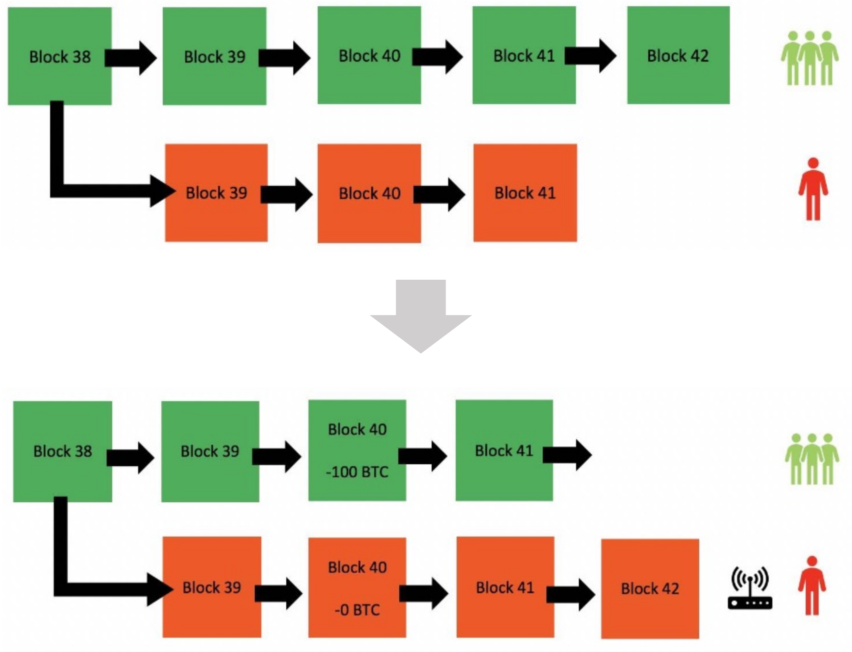
➢TPS

Transaction confirming throughput measured as transaction-per-second (TPS)

4k TPS   256k TPS   ~20 TPS

➢51% attack





Problem & Goal

- Problem

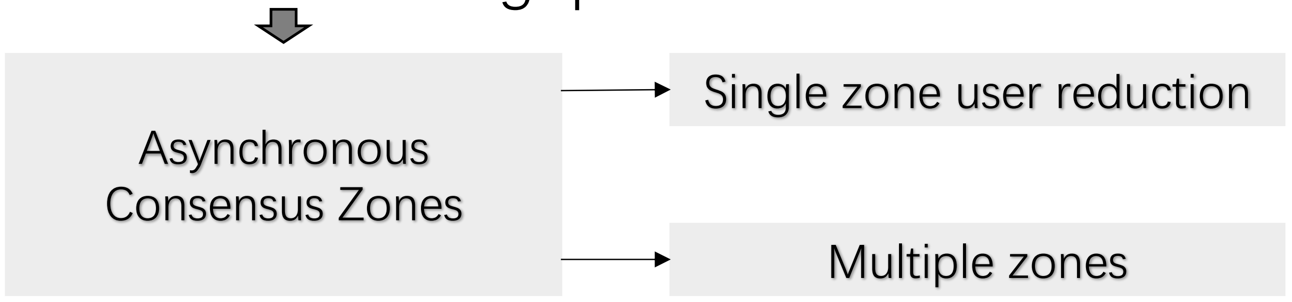
  low throughput has significantly hindered the scalability and usability of cryptocurrency systems for increasing numbers of users and transactions

- Goal

  high throughput without weakening decentralization or security

Challenges

- ➢How to increase throughput for blockchain



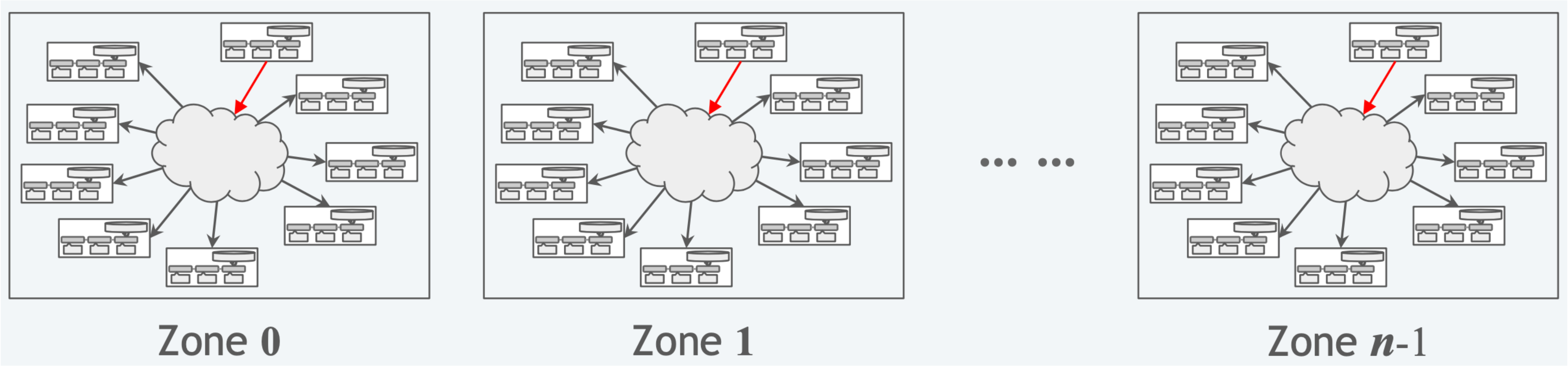
- ➢How to efficient handling of cross-zone transactions

- ➢How to prevent 51% attacks against a single zone

Asynchronous Consensus Zones

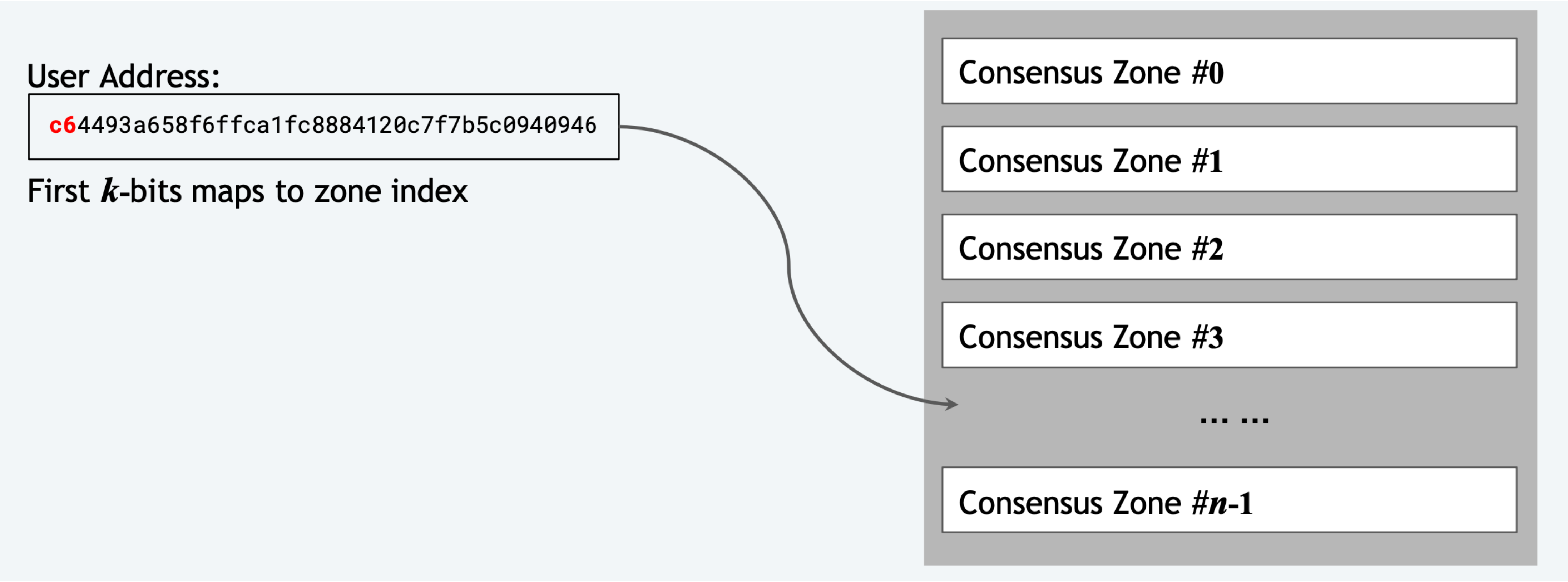
Divide the blockchain network into multiple independent and parallel Zones

- Build a blockchain within each consensus zone
- Miners mine in their own Zone through PoW



Asynchronous Consensus Zones

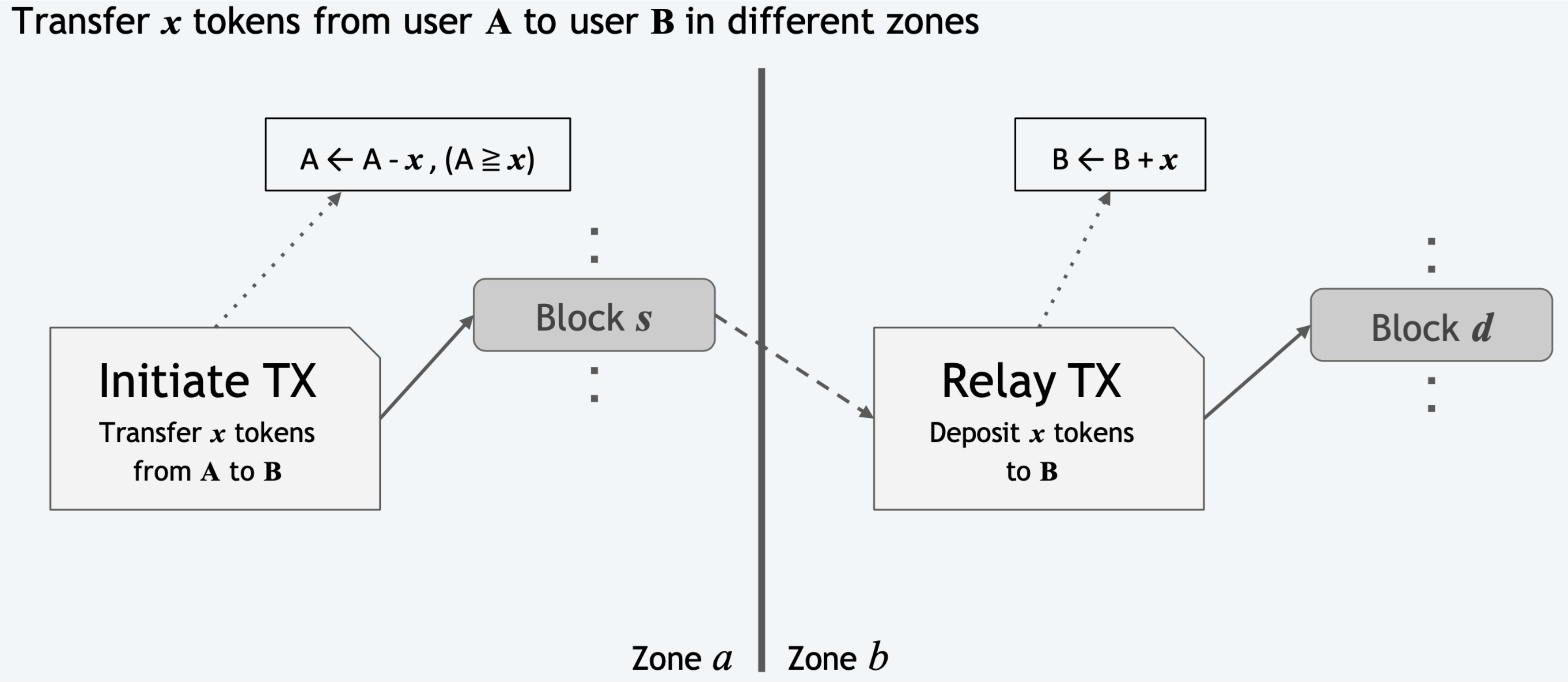
Zone Count：$n = 2^k$



Cross-Zone Transactions - transaction process

Complete transaction = Initiate TX + Relay TX

1. Initiate transaction in zone A was successfully packaged
2. Relay TX is passed to zone B
3. The transaction is packaged in zone B

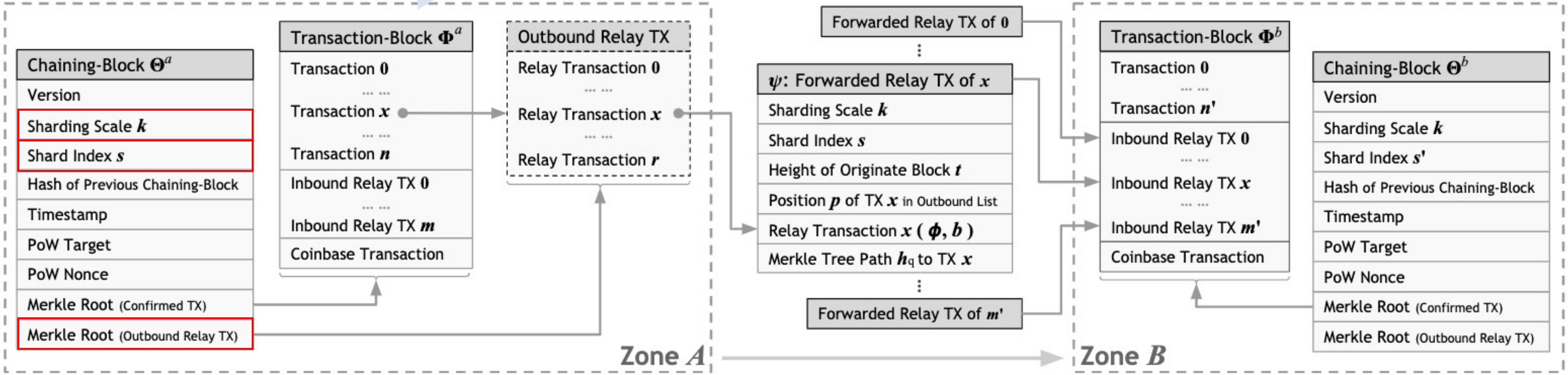


Cross-Zone Transactions - block design

- Chaining-Block : the chain formation and the PoW verification
- Transaction-Block : carrying actual confirmed transactions
- Outbound Relay : collection of all Relay TX

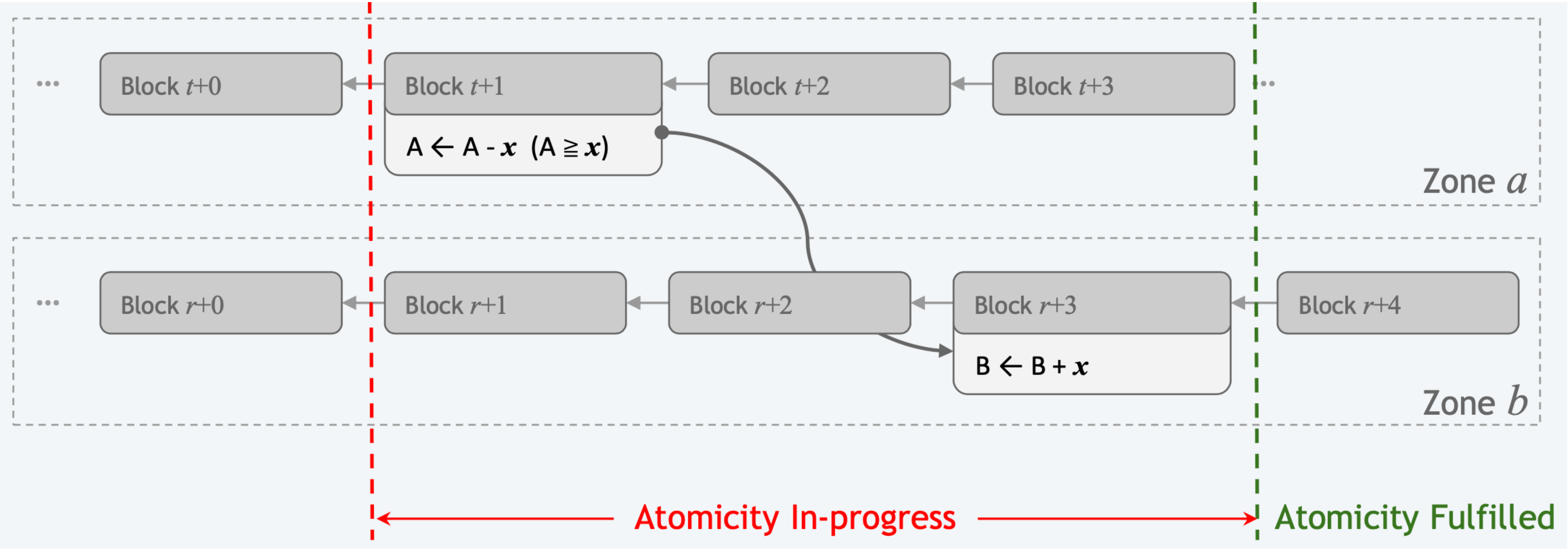
= the previous block body

difference



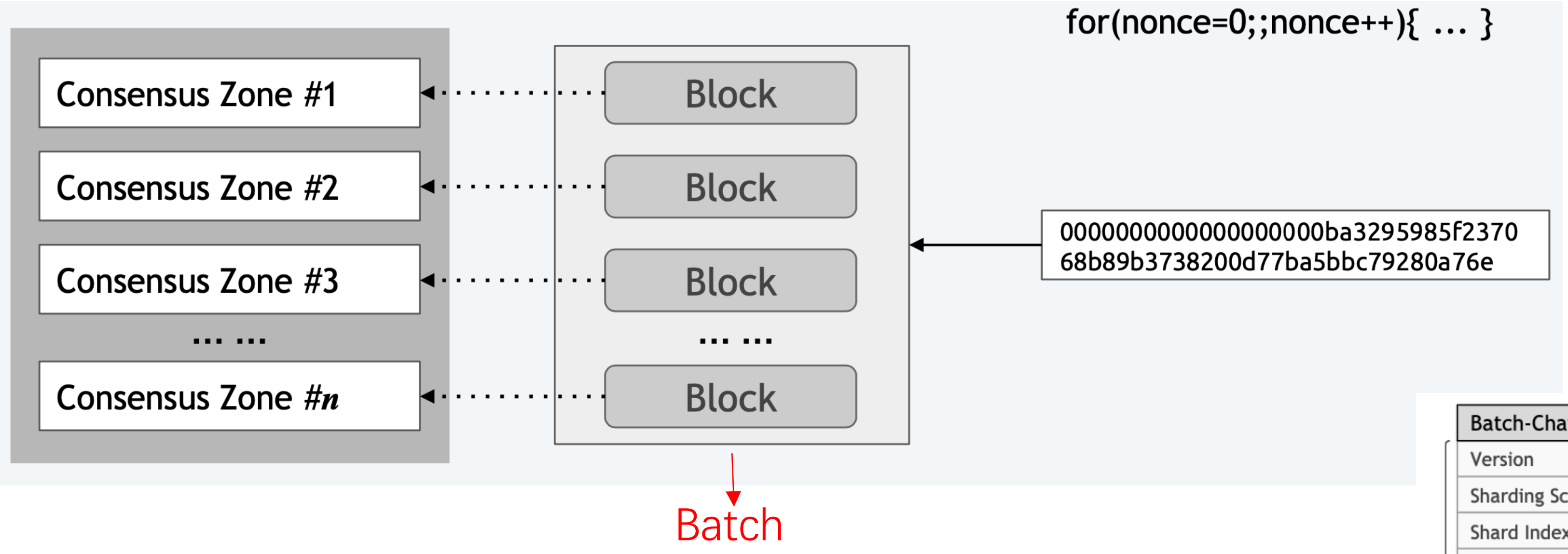
Cross-Zone Transactions - guaranteed atomicity

- Relay Tx will never expire before being passed to the target zone
- In case of accidental loss, Relay TX can be rebuilt from the original Zone

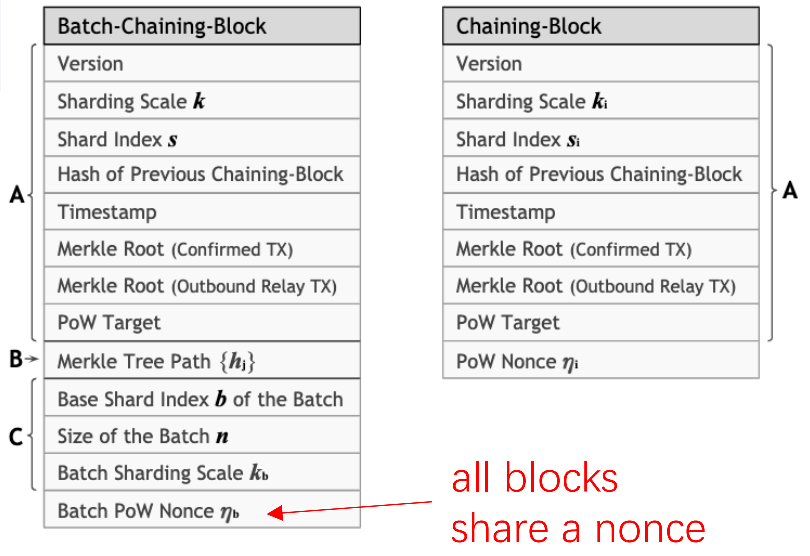


Chu-ko-nu Mining

Main idea : a miner use **a single PoW solution** to create **multiple blocks** at different zones simultaneously, but **no more than one block per-zone**



- For honest miners : can get more rewards
- For malicious miners : competing with **more miners**, when the batch size is large enough, the effect is similar to mining in the whole network



Evaluation-Transaction distribution & Throughput

- Transaction distribution

  -Transactions handled in each zone are balanced

  -Single Address Hotspot

  e.g., a deposit address of a large cryptocurrency exchange

  0x3f5CE5FBFe3E9af3971dD833D26bA9b5C936f0bE (Binance)

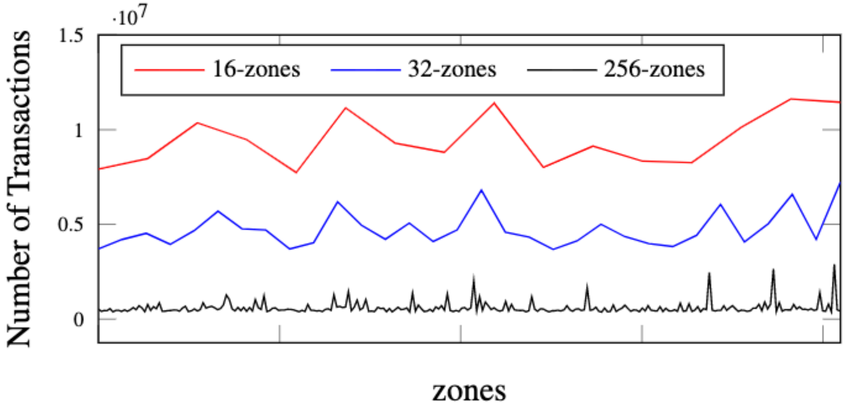


Figure 7: Transaction distribution across zones.

- Throughput

  -achieves up to 11,694.89 TPS when there are 2,048 zones

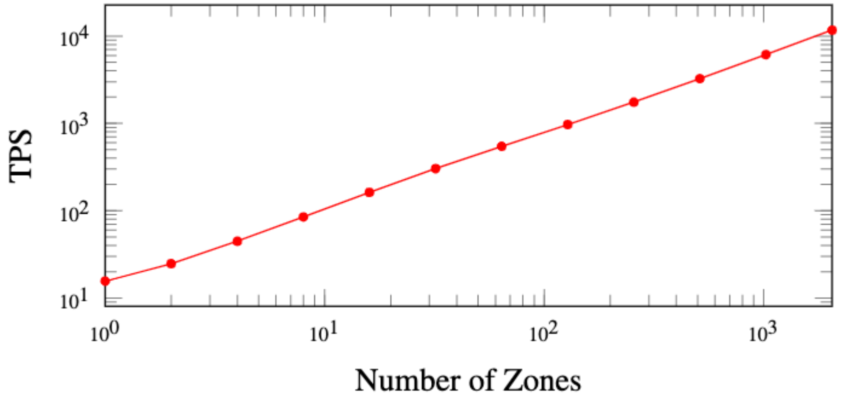


Figure 6: Linear scaling out with multiple zones.

Evaluation-Overhead

- Proportion of cross-zone transactions

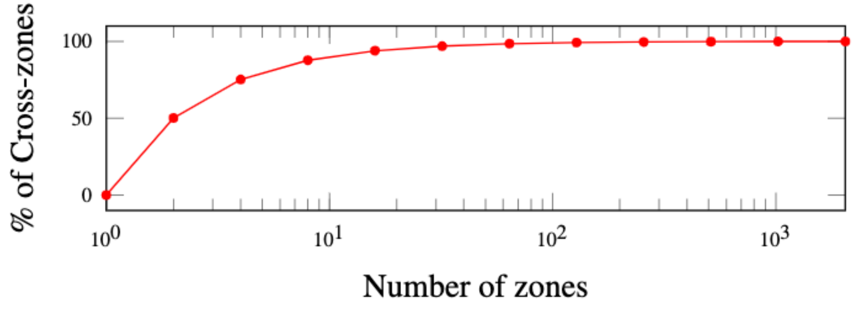


Figure 8: Percentage of cross-zone transactions, which approaches to 100%. Almost every original transaction produced a relay transaction.

- Storage overhead

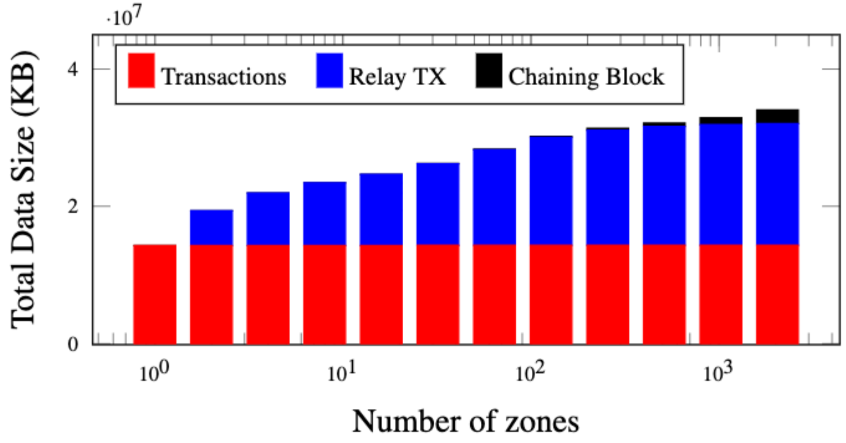
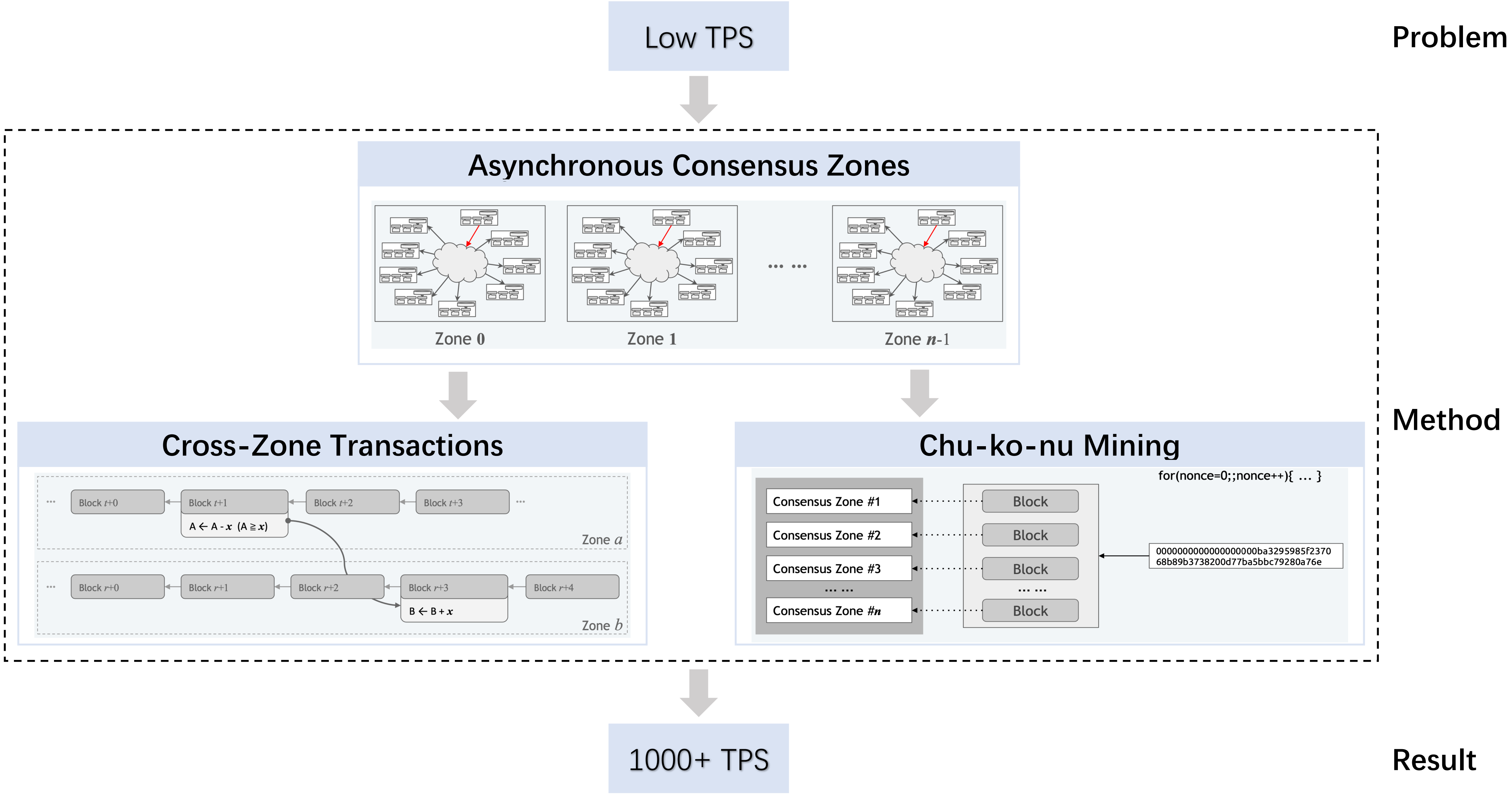


Figure 9: Sizes of the blockchain data in the entire network.

Conclusion



Low TPS
Problem
Asynchronous Consensus Zones
Zone 0
Zone 1
Zone n-1
Method
Cross-Zone Transactions
Block t+0
Block t+1
Block t+2
Block t+3
A ← A - x (A ≥ x)
Zone a
Block r+0
Block r+1
Block r+2
Block r+3
Block r+4
B ← B + x
Zone b
Chu-ko-nu Mining
for(nonce=0;;nonce++){ … }
Consensus Zone #1
Consensus Zone #2
Consensus Zone #3
Consensus Zone #n
Block
0000000000000000000ba3295985f2370
68b89b3738200d77ba5bbc79280a76e
1000+ TPS
Result