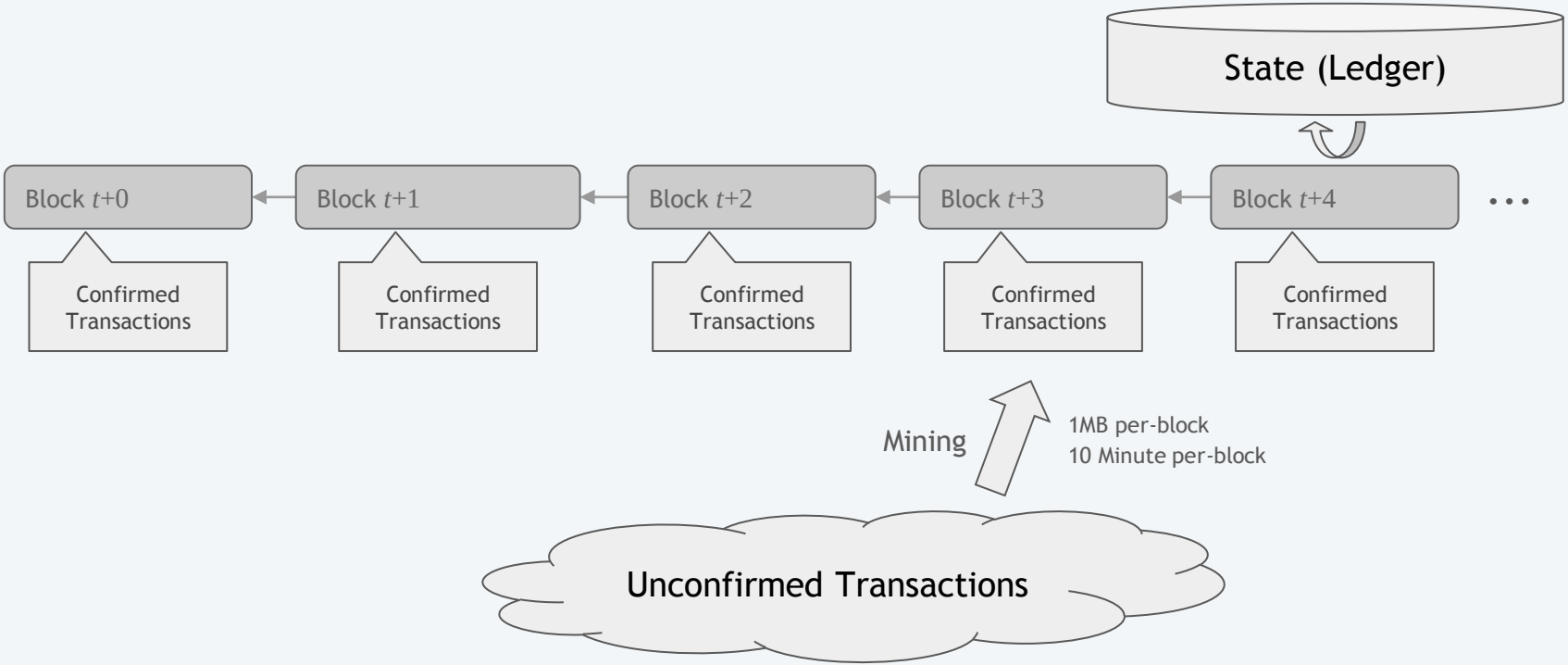
Monoxide

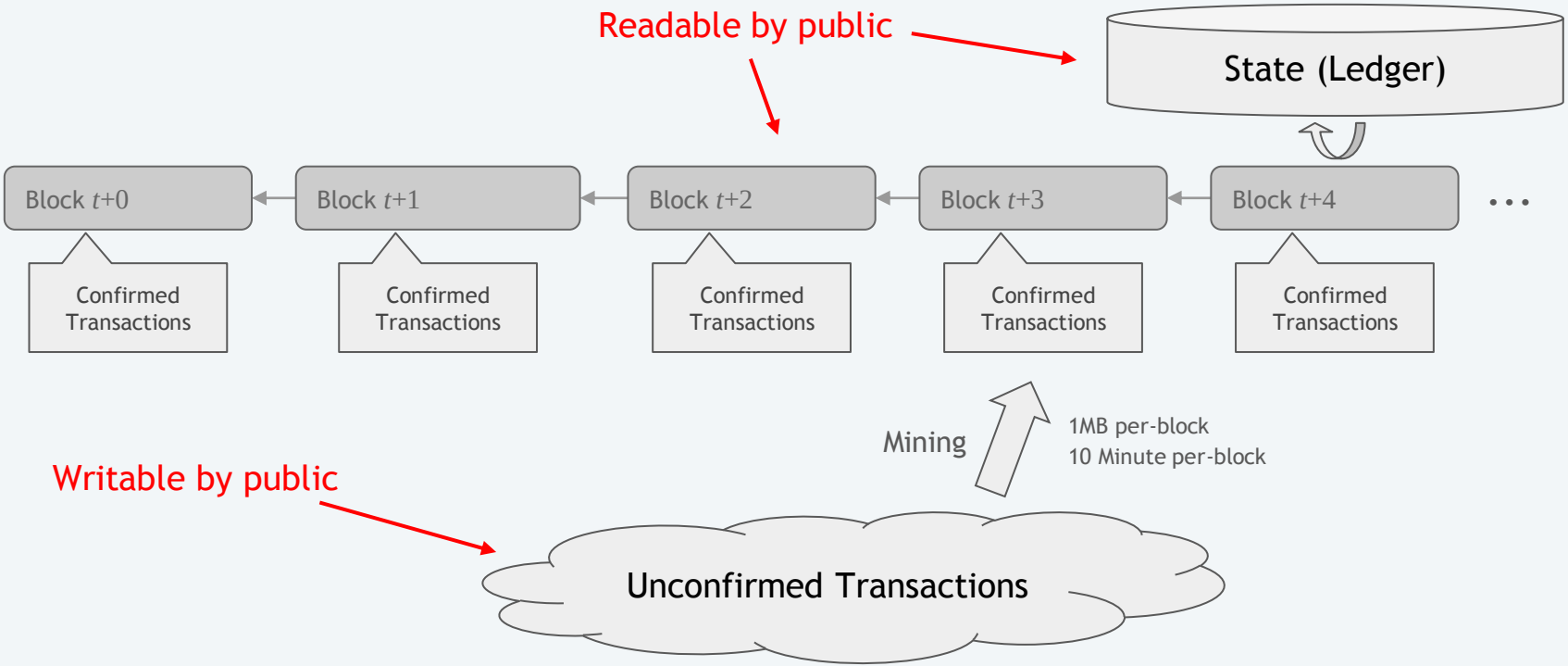
Scale out Blockchains with Asynchronous Consensus Zones

Jiaping Wang, Hao Wang
Sinovation Ventures
ICT/CAS
The Ohio State University

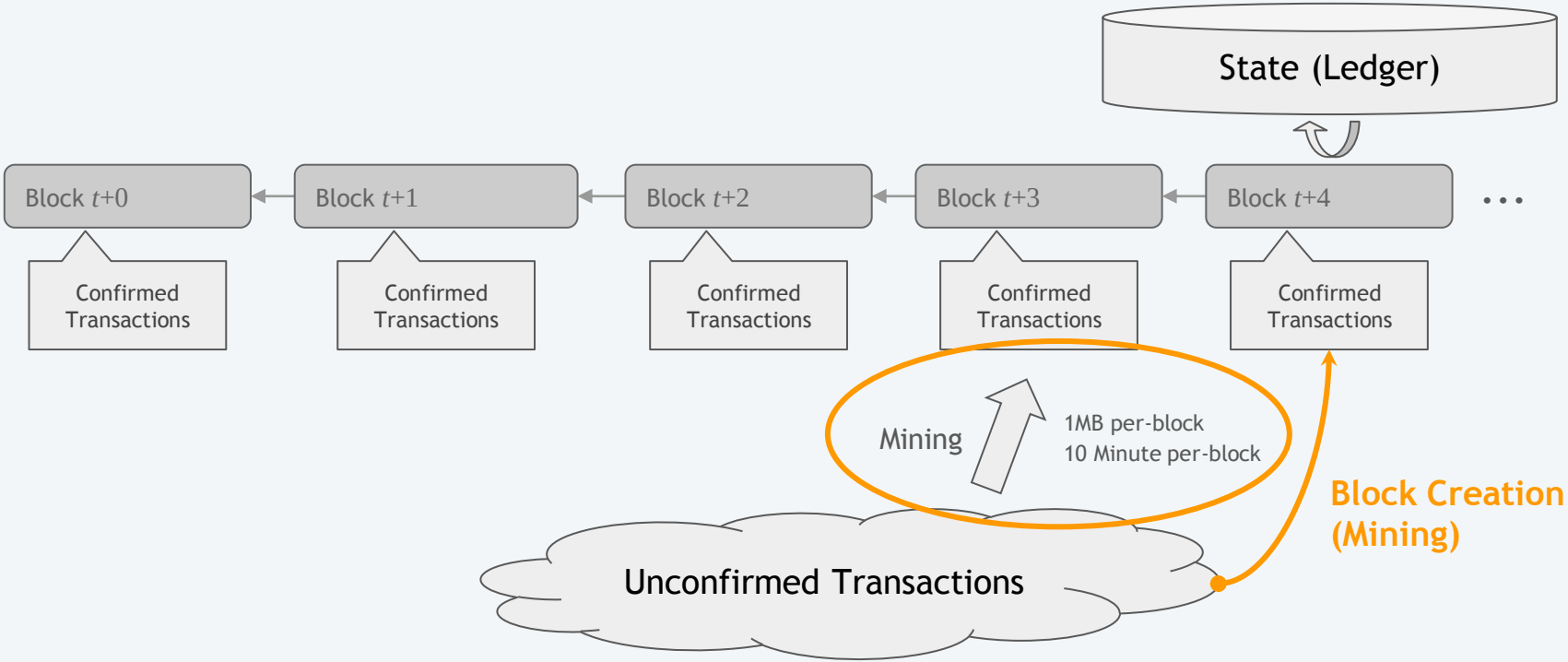
Public Blockchain



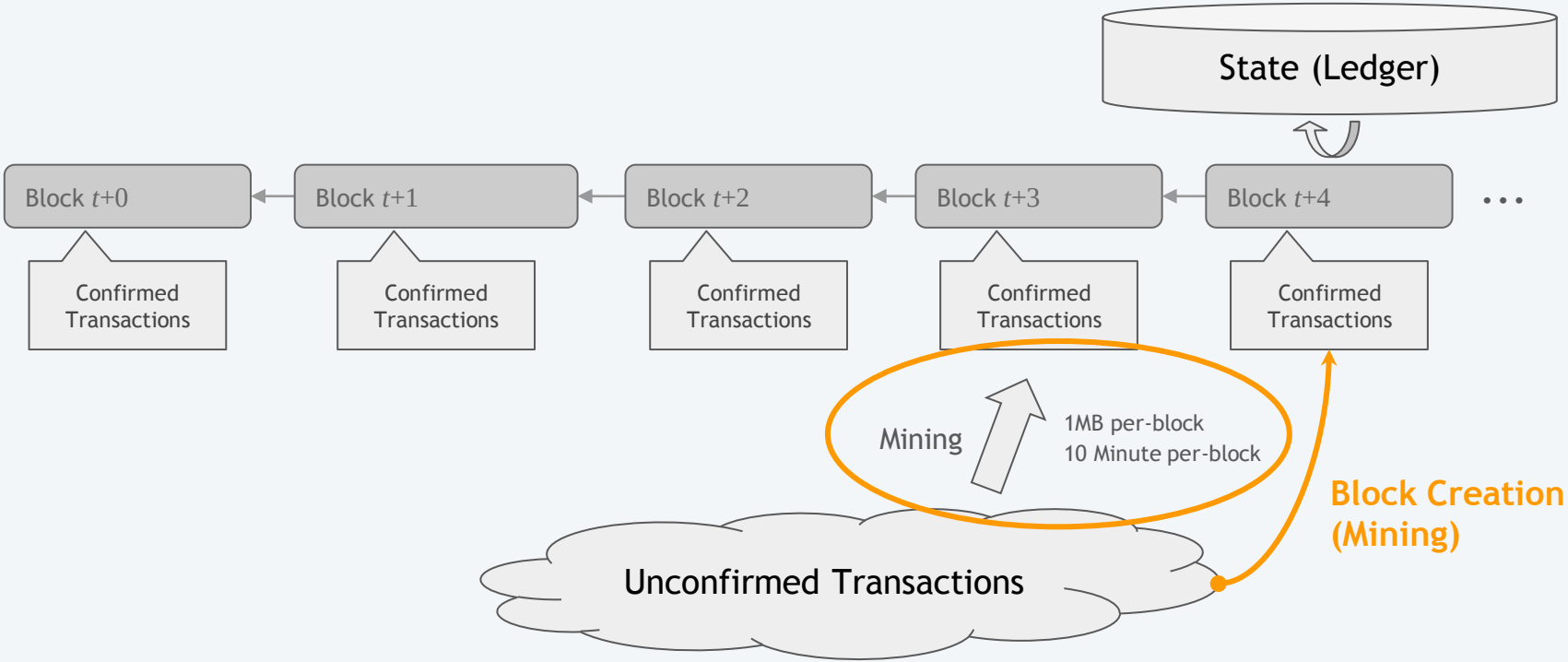
Public Blockchain



Public Blockchain



Public Blockchain



Decentralized Communication: IP & IP Routing
Decentralized Storage: BitTorrent / DHT

Decentralized Computing

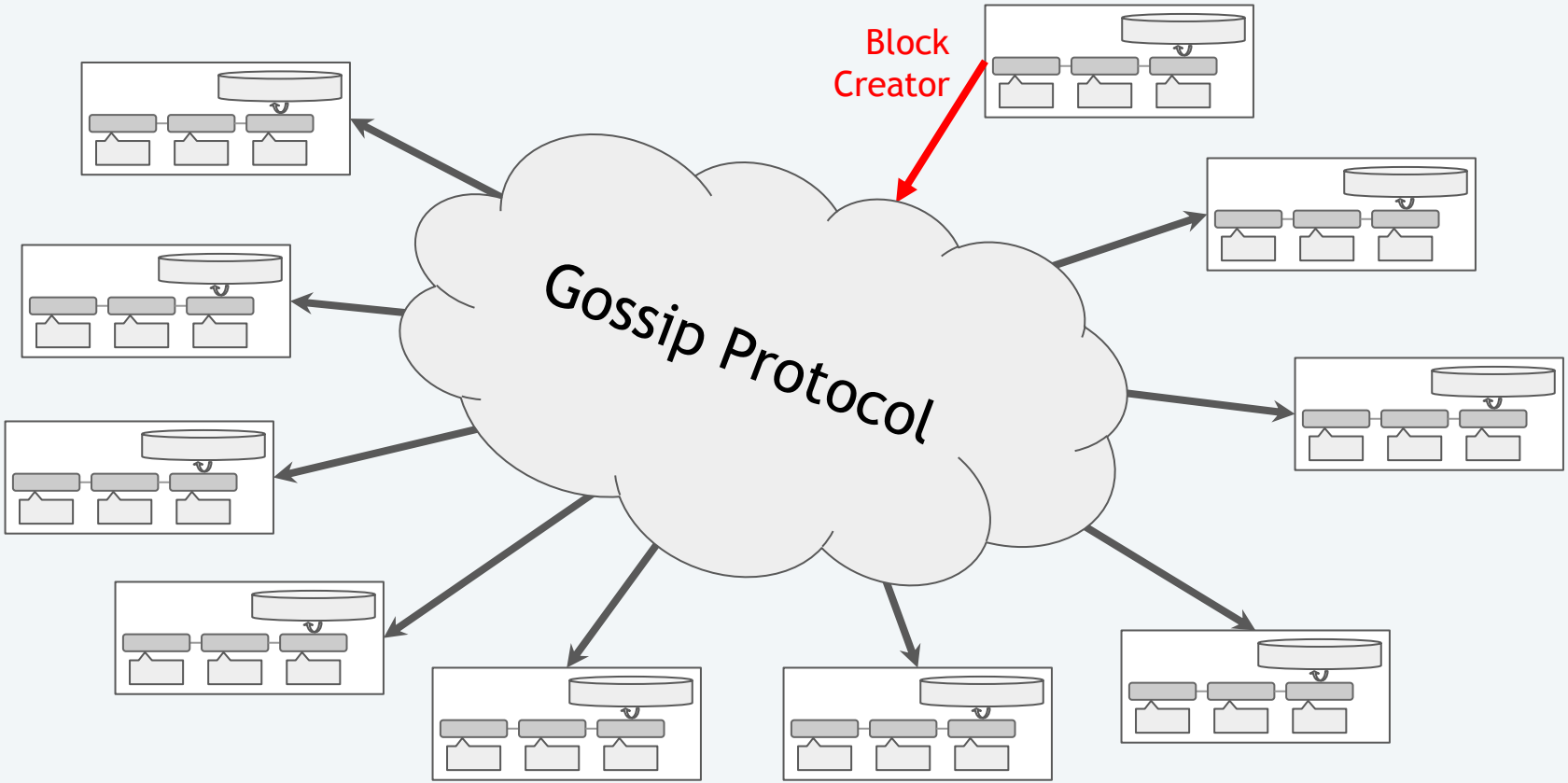
- Immutable Logic, faithful execution
- Trustworthy result, verifiable trustlessly
- Unstoppable, no manipulation
- Unblockable, permissionless

Decentralized Communication: IP & IP Routing
Decentralized Storage: BitTorrent / DHT

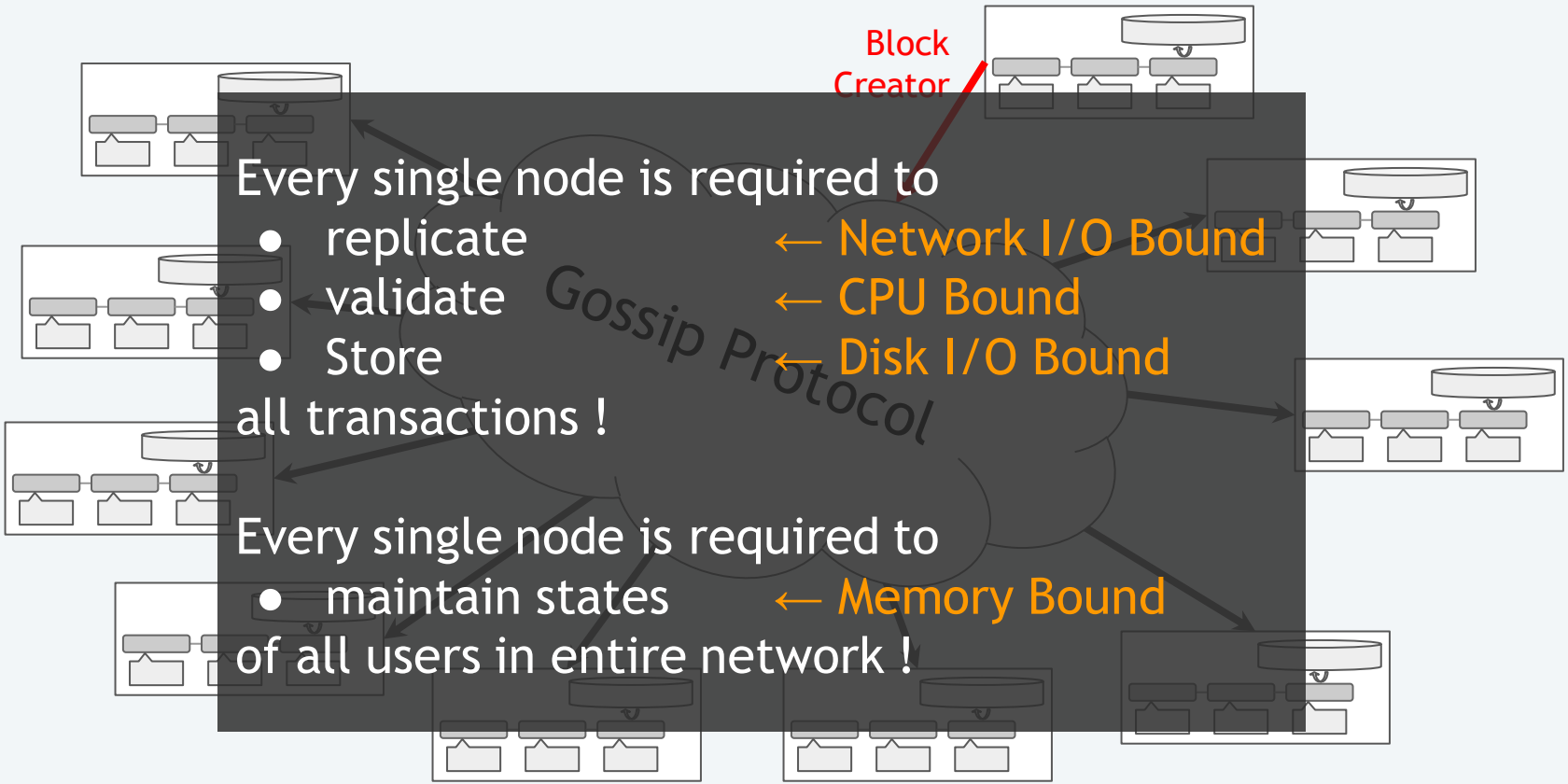
Decentralized Computing

- Immutable Logic, faithful execution
- Trustworthy result, verifiable trustlessly
- Unstoppable, no manipulation
- Unblockable, permissionless

Not Scalable: Low TPS

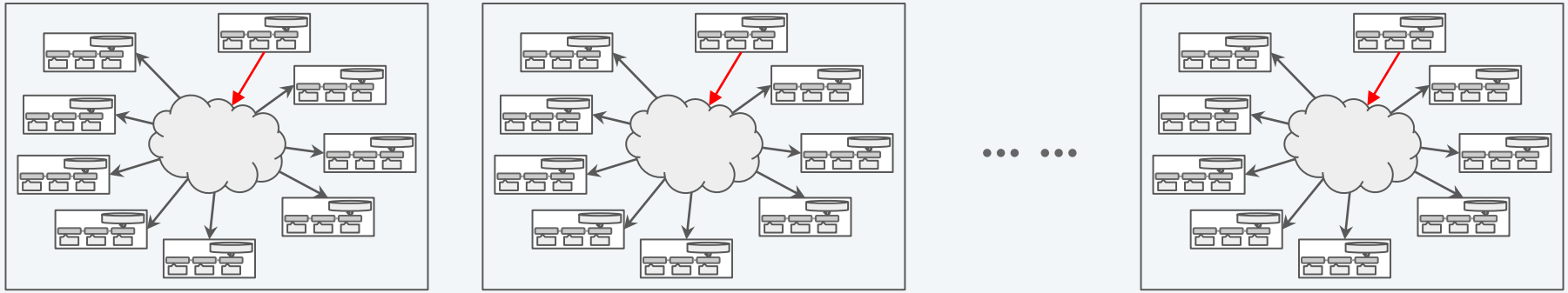


Not Scalable: Low TPS



Asynchronous Consensus Zones

- Consensus Zones: Multi-instantiation of independent blockchain systems
- Partitioning workloads of the entire network, distribute to zones
- Parallelize block creation and transaction handling
- Linear scalable as the entire network is divided into more zones



SYSTEM DESIGN

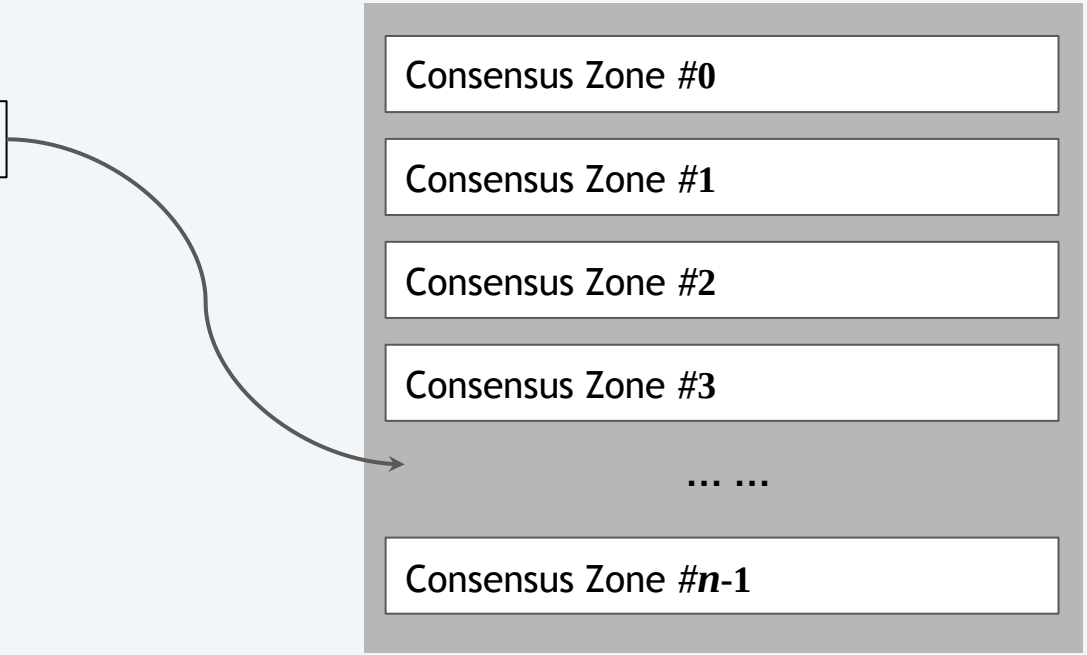
Partitioning in Consensus Zones

Zone Count: $n=2^k$

User Address:

`c64493a658f6ffca1fc8884120c7f7b5c0940946`

First k-bits maps to zone index



Partitioning in Consensus Zones

Zone Count: $n=2^k$

User Address:

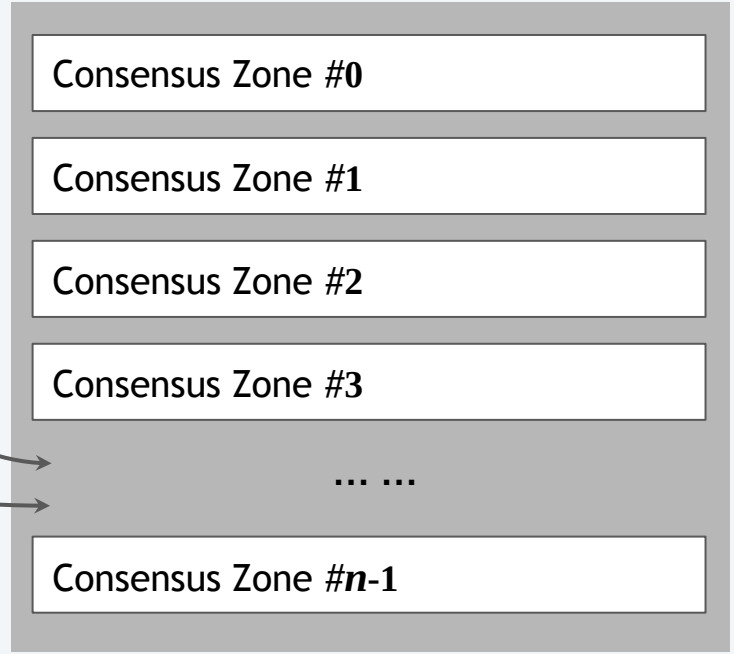
`c64493a658f6ffca1fc8884120c7f7b5c0940946`

First k-bits maps to zone index

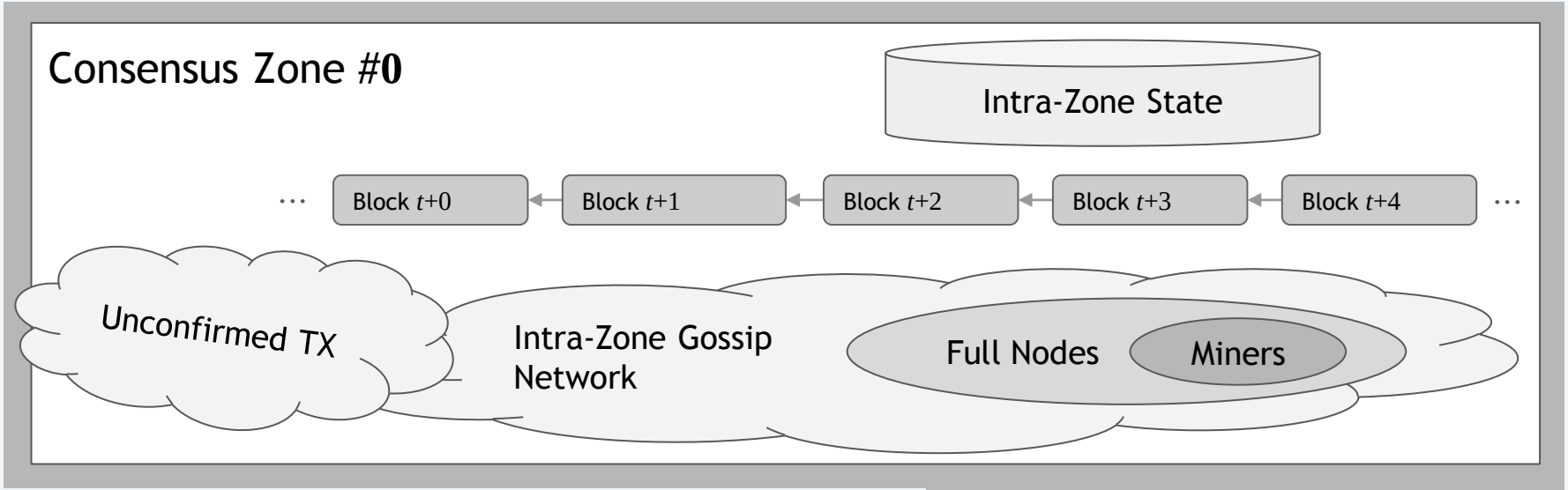
Transaction:

```
From:5e032243d507c743b061ef021e2ec7fcc6d3ab89
To:  eba290cf248cb14442a071fbcb58a9cc5dcde28e
```

First k-bits of **From** maps to zone index



Consensus Zones



Zone isolates

- Mining competition and chain growth
- State (ledger) for intra-zone users only
- Unconfirmed TX (mempool)
- Gossip network

Consensus Zone #1

Consensus Zone #2

... ...

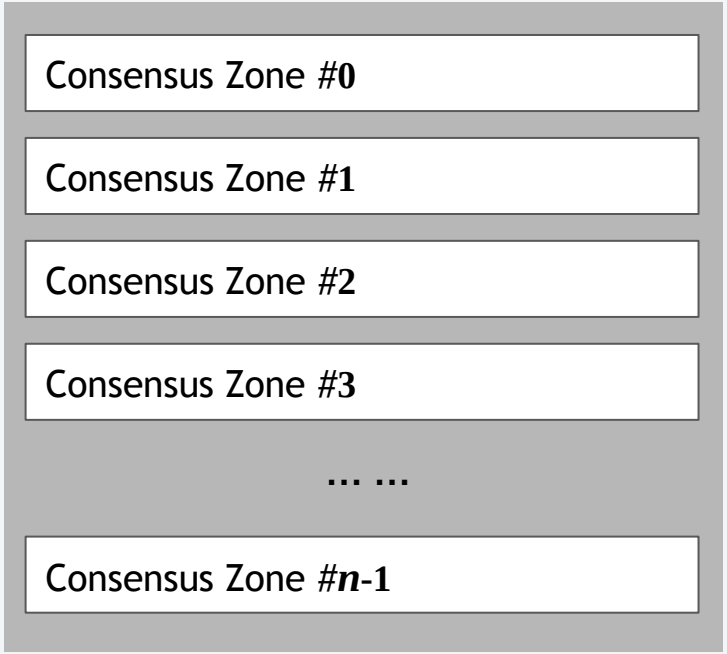
Consensus Zone #n-1

Consensus Zones

Scalability

✓ Linear scaled capacity: CPU, Memory, Disk I/O

× Throughput ?? Cross-zone transaction ??



Consensus Zones

Scalability

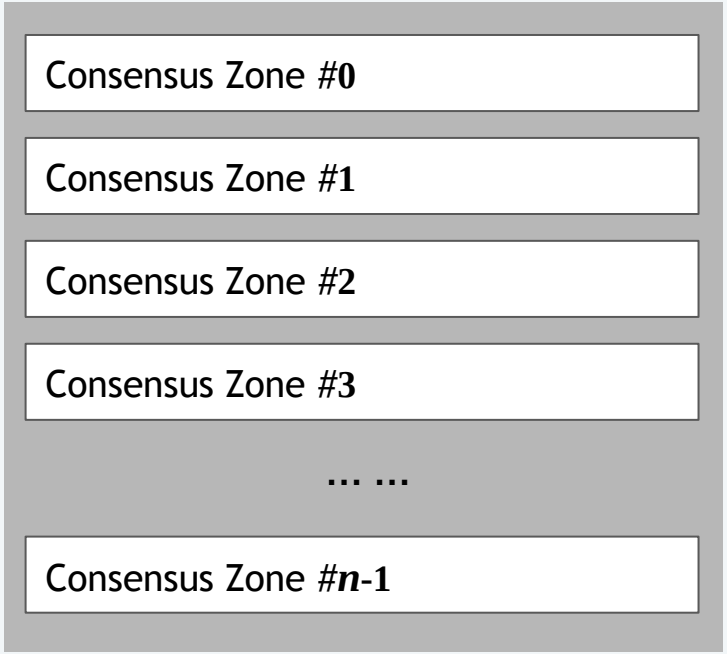
✓ Linear scaled capacity: CPU, Memory, Disk I/O

× Throughput ?? Cross-zone transaction ??

Security

× Attack bar: mining power dilution ??

✓ Sybil resistant



Consensus Zones

Scalability

✓ Linear scaled capacity: CPU, Memory, Disk I/O

× Throughput ?? Cross-zone transaction ??

Security

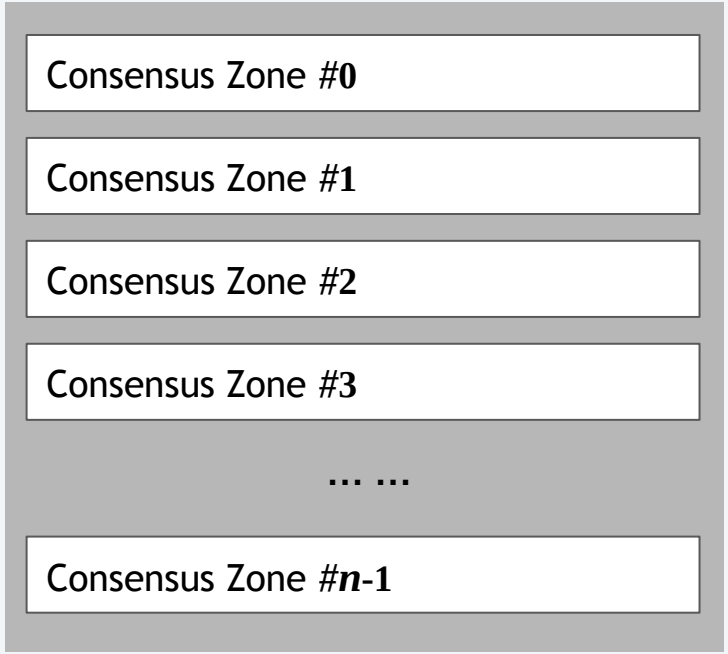
× Attack bar: mining power dilution ??

✓ Sybil resistant

Decentralization

✓ Permissionless mining

✓ Low barrier of participate (full nodes)



Consensus Zones

Scalability

✓ Linear scaled capacity: CPU, Memory, Disk I/O

× Throughput ?? Cross-zone transaction ??

Security

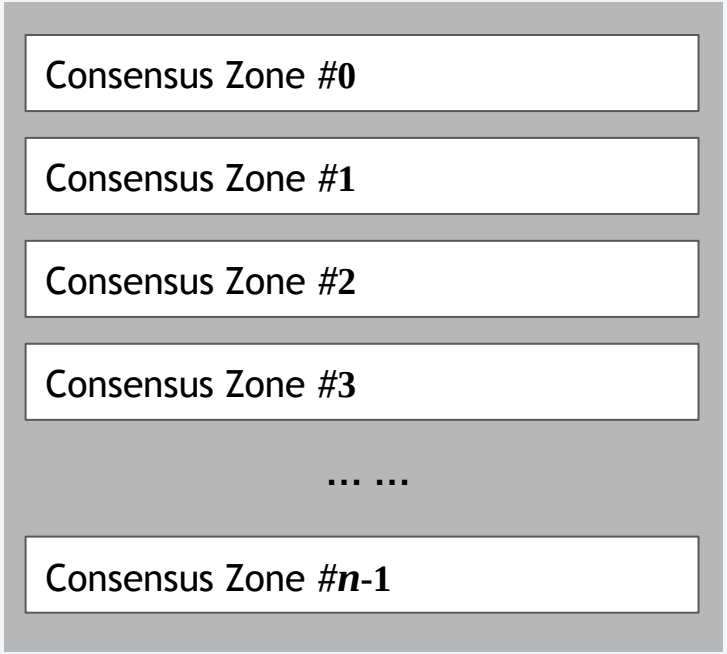
× Attack bar: mining power dilution ??

✓ Sybil resistant

Decentralization

✓ Permissionless mining

✓ Low barrier of participate (full nodes)



Contributions

#1 Efficient Cross-Zone Transaction Handling

Atomic Transfer: Transfer x tokens from user $\mathbf{A}$ to user $\mathbf{B}$ from different zones

Conditional Operation: $A \leftarrow A - x$, $(A \geqq x)$

Unconditional Operation: $B \leftarrow B + x$

Contributions

#1 Efficient Cross-Zone Transaction Handling

Atomic Transfer: Transfer x tokens from user $\mathbf{A}$ to user $\mathbf{B}$ from different zones

Conditional Operation: $A \leftarrow A - x$, $(A \geqq x)$

Unconditional Operation: $B \leftarrow B + x$

#2 Mining Power Diluted with Multiple Zones

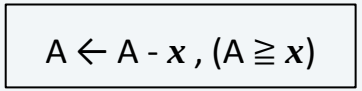
Focused Attack on a Specific Individual Zone (1% attack)

CROSS-ZONE TRANSACTION

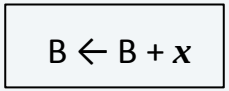
Cross-Zone

Payment Transaction

Transfer x tokens from user $\mathbf{A}$ to user $\mathbf{B}$ in different zones



Conditional Operation
Order-dependent

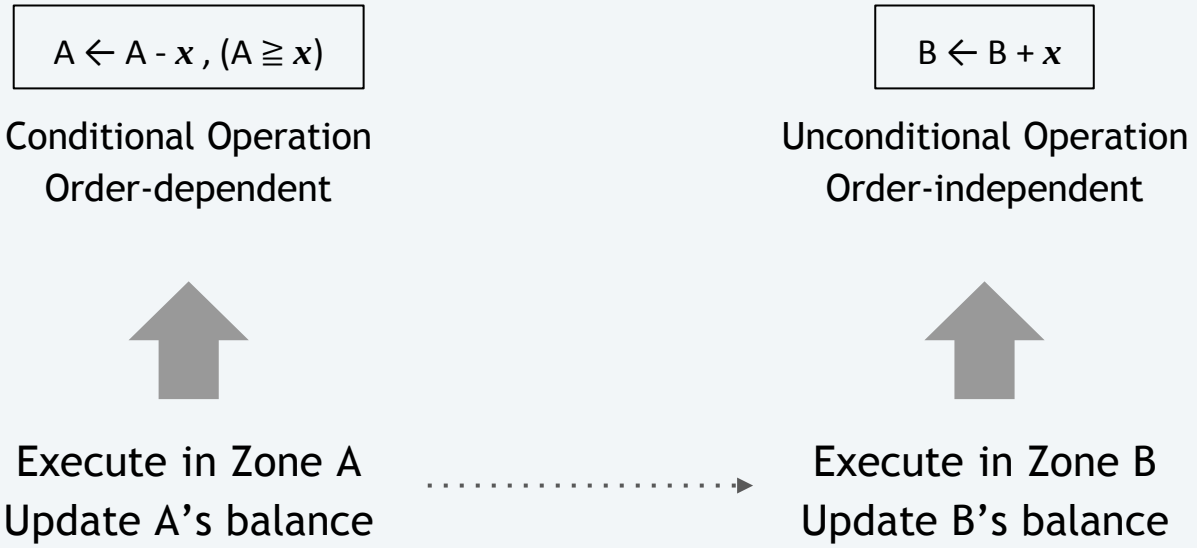


Unconditional Operation
Order-independent

Cross-Zone

Payment Transaction

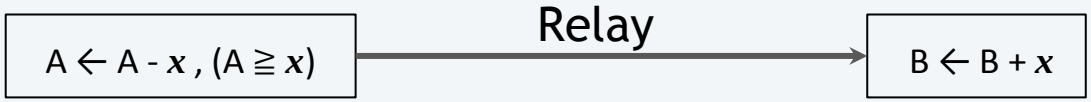
Transfer x tokens from user $\mathbf{A}$ to user $\mathbf{B}$ in different zones

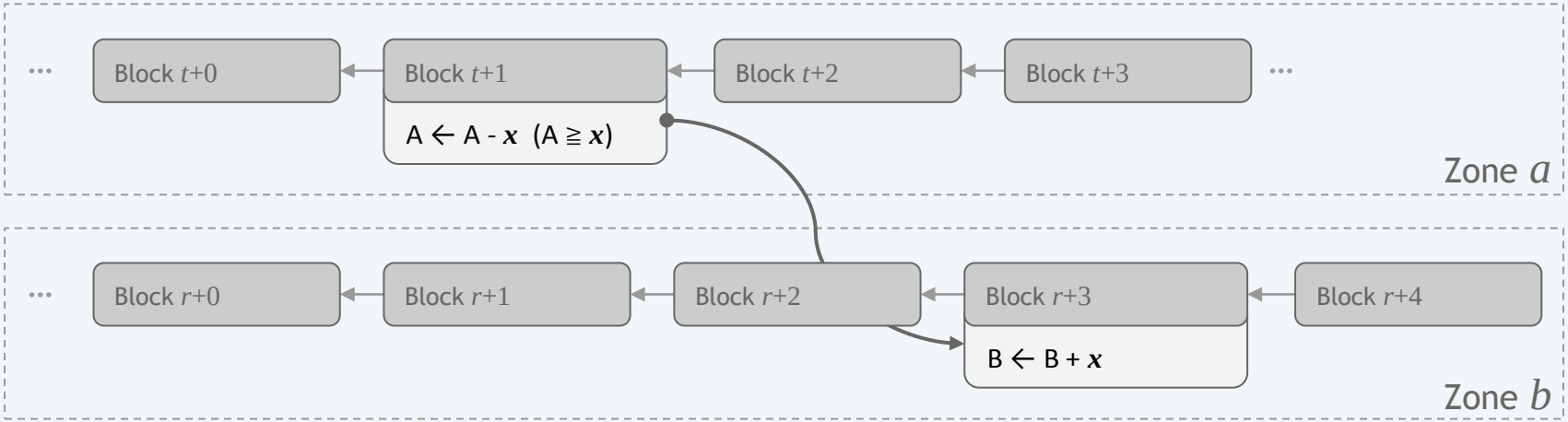


Cross-Zone

Payment Transaction

Transfer x tokens from user $\mathbf{A}$ to user $\mathbf{B}$ in different zones

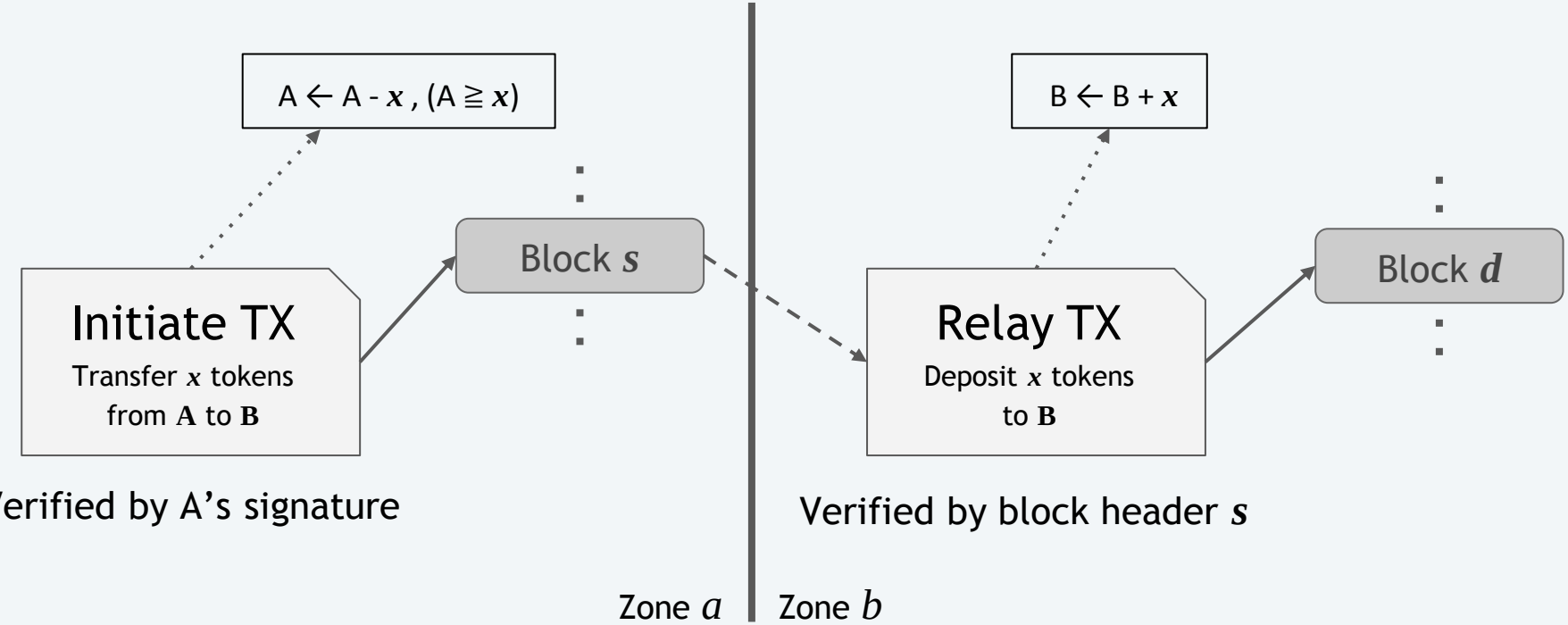




Message Passing

Payment Transaction = Initiate TX + Relay TX

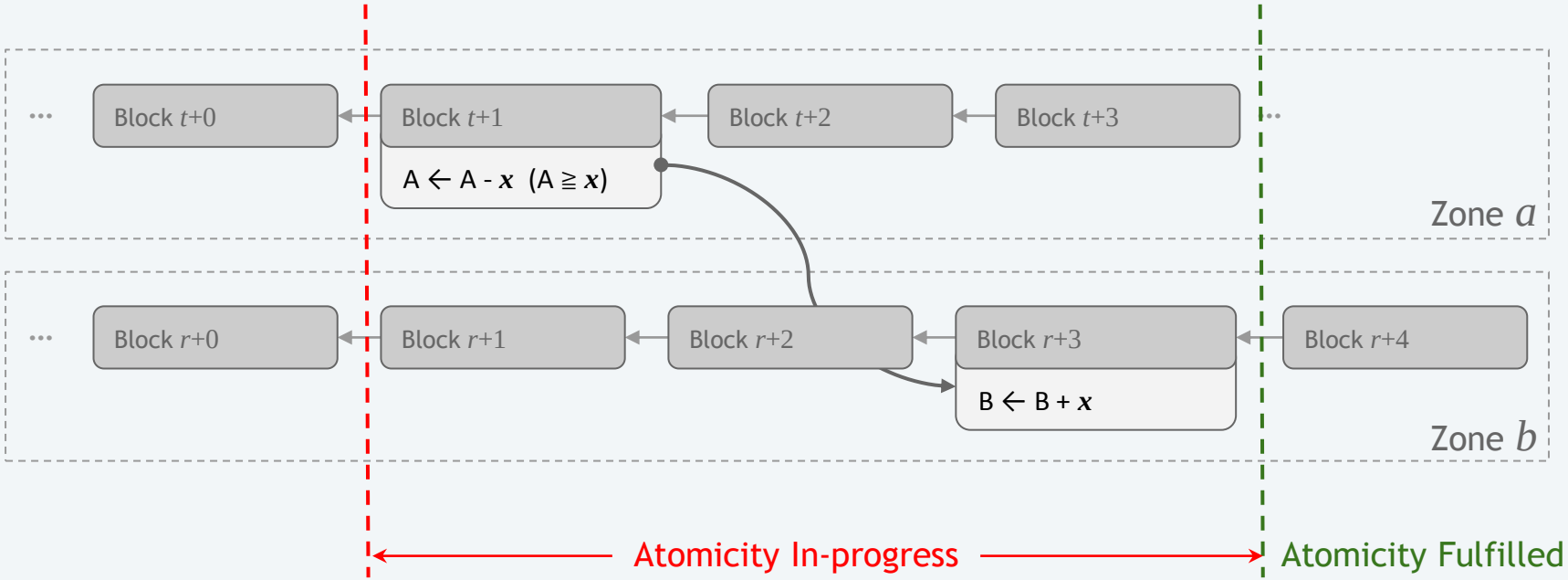
Transfer x tokens from user $\mathbf{A}$ to user $\mathbf{B}$ in different zones



Eventual Atomicity

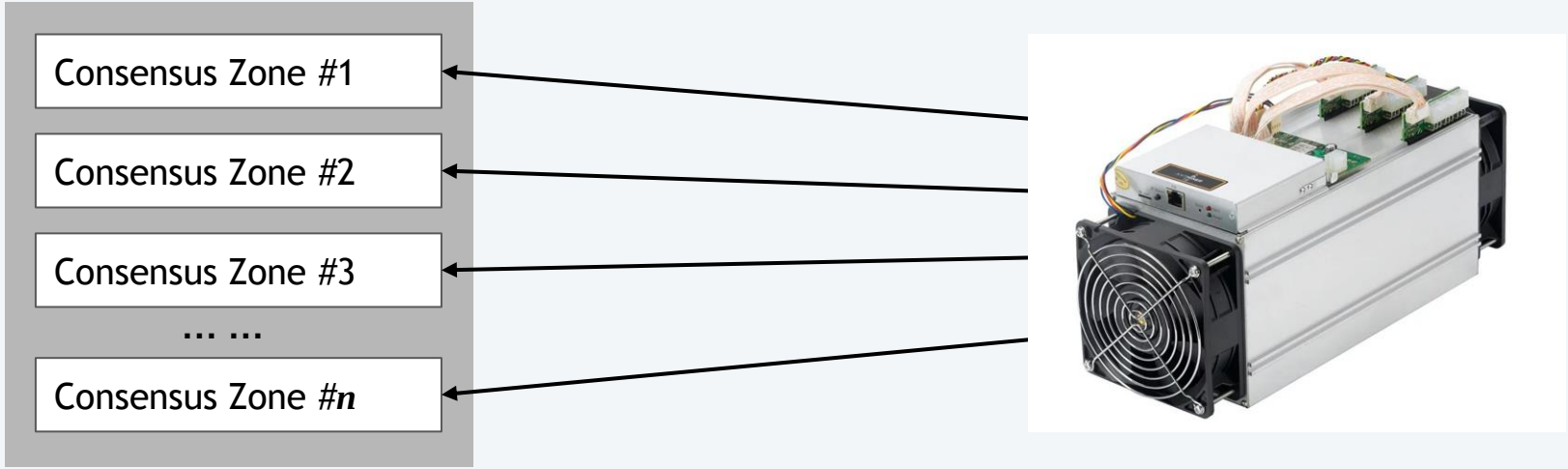
Payment Transaction = Initiate TX + Relay TX

Transfer x tokens from user $\mathbf{A}$ to user $\mathbf{B}$ in different zones

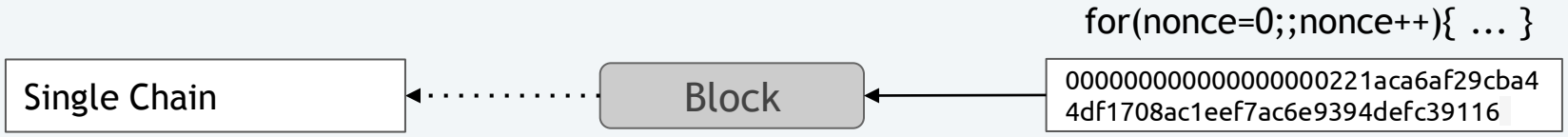


MINING POWER DILUTION

Security Issue: Single-Zone Focused Attack



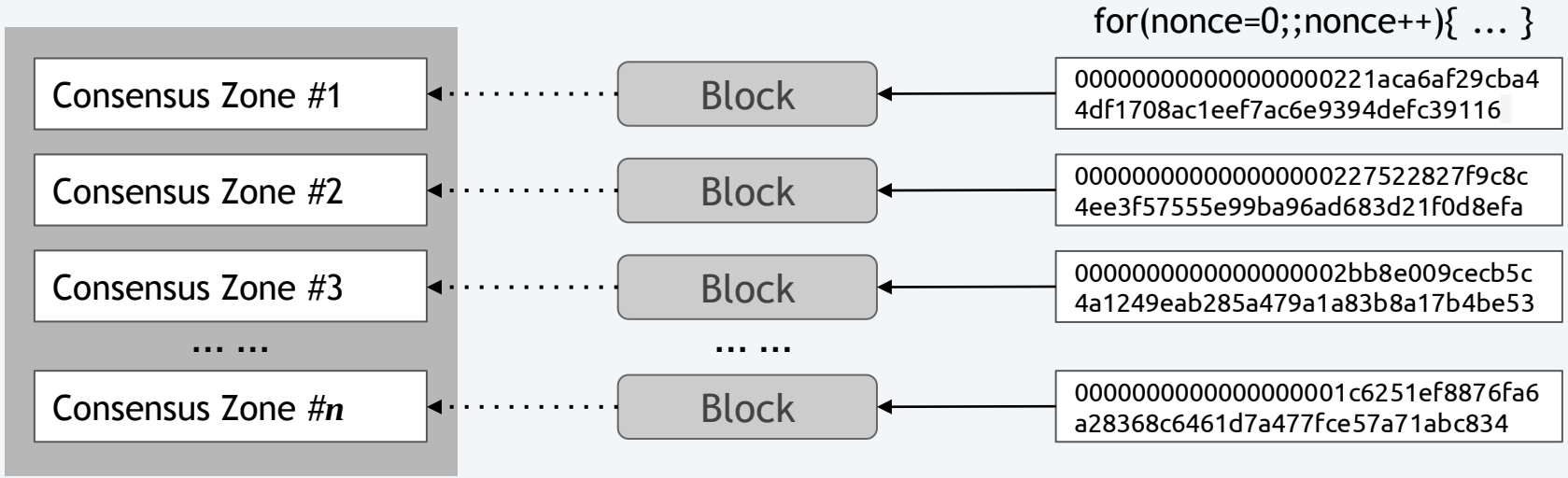
Effective Mining Power



Total Hashrate: t hash/sec

Total Effective Mining Power: t hash/sec

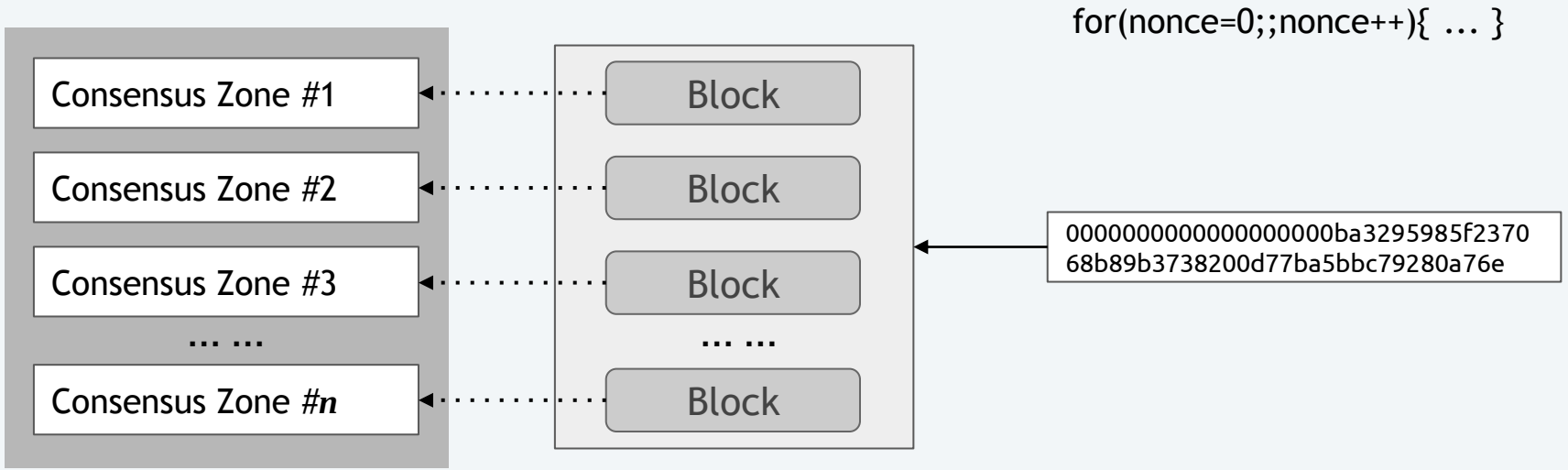
Effective Mining Power



Total Hashrate: ***t*** hash/sec

Total Effective Mining Power: ***t*** hash/sec

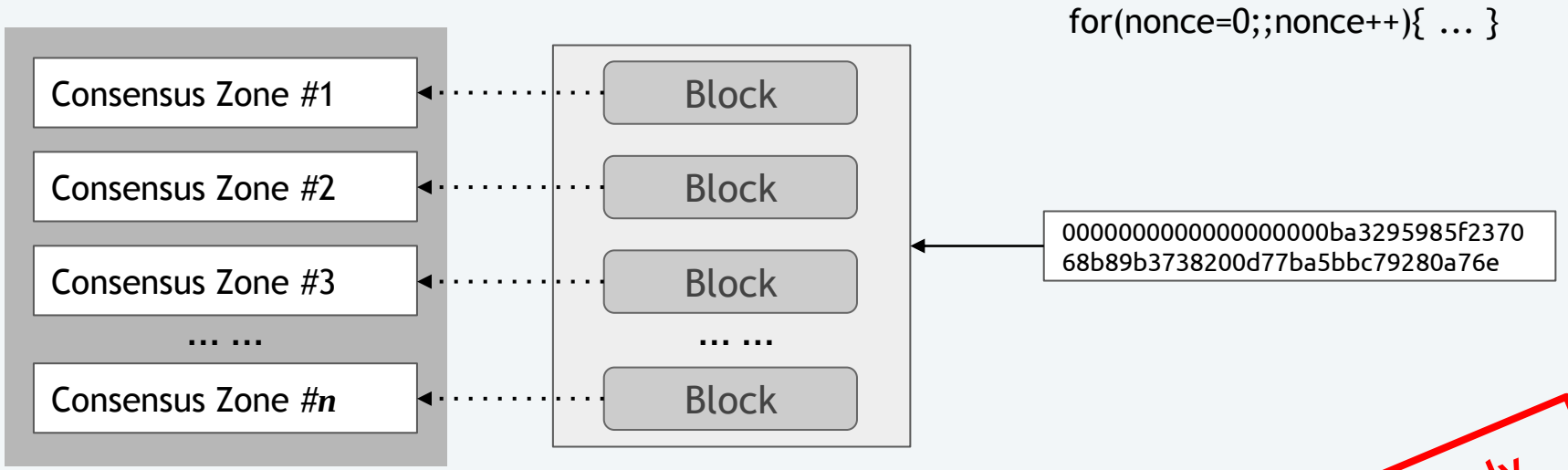
Chu-ko-nu Mining (诸葛连弩)



Total Hashrate: t hash/sec

Total Effective Mining Power: $t \times n$ hash/sec

Chu-ko-nu Mining (诸葛连弩)



Total Hashrate: t hash/sec

Total Effective Mining Power: $t \times n$ hash/sec

Enforced to be evenly distributed across zones !!

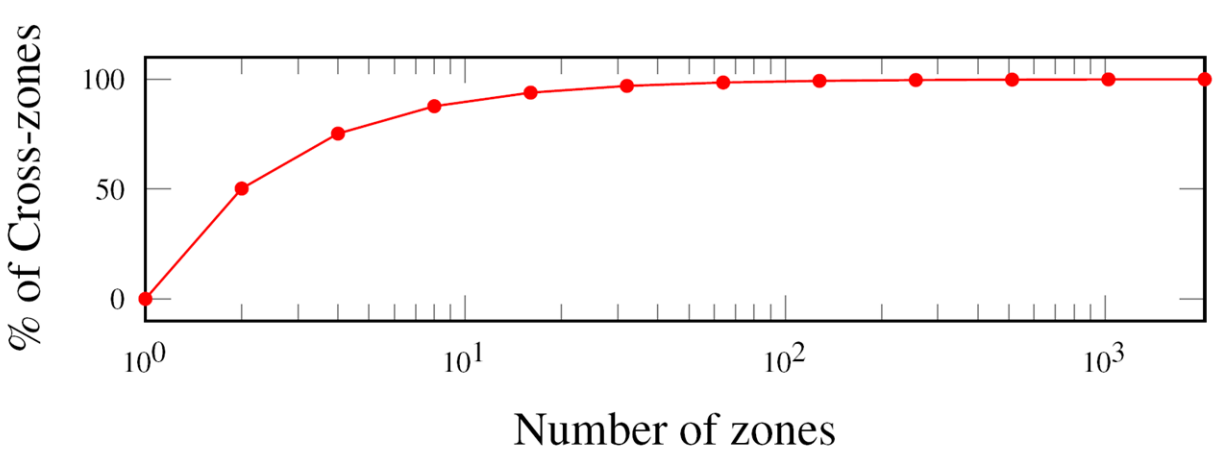
Experimental Result

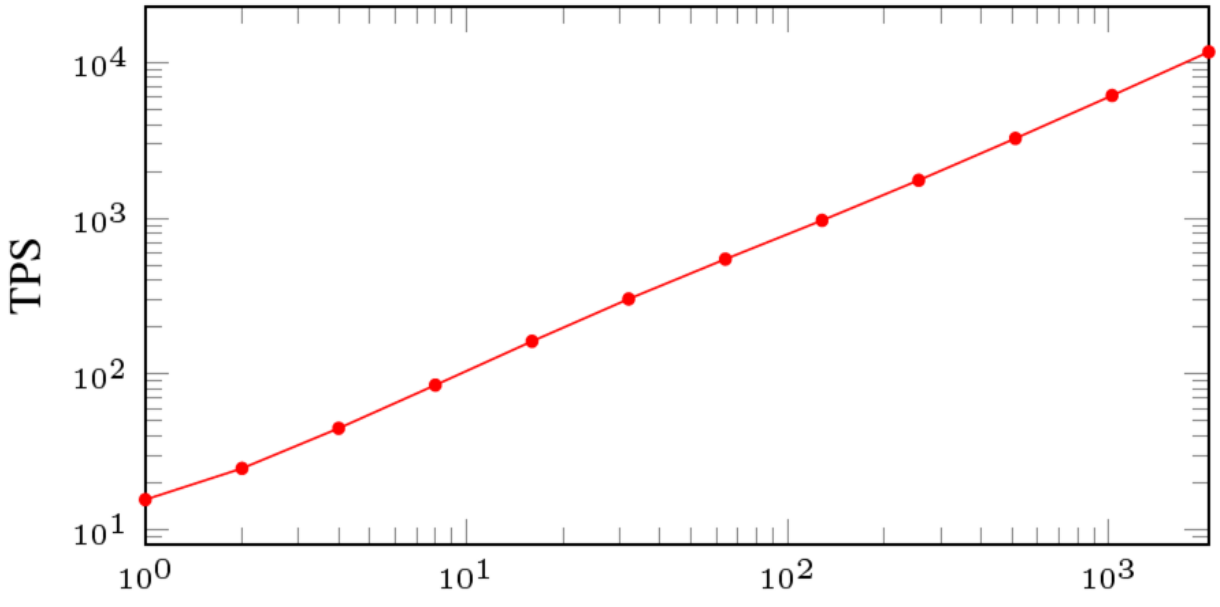
Experiment Setup

Playback ERC20 historical payment transactions

16.5 M Addresses
75.8 M Transactions

30Mbps per-node
15.6 TPS per-zone
1 to 2048 zones





Takeaways

- Monoxide achieves scalability, security and decentralization at the same time
- Monoxide Partitions all workload
  - communication, transaction processing, state representation, history archiving
  - Network bandwidth, computing power, memory size, disk I/O

- Eventual Atomicity: Efficient cross-zone transaction handling
- Chu-ko-nu Mining: Security guarantee for individual zones

- We achieved 10K TPS, and Million TPS is possible
- Neutral to actual consensus algorithm used in zones

Our project will be open source and offer the new generation blockchain platform at *https://monoxide.io* **Twitter: @monoxide_io**

Monoxide

Scale out Blockchains with Asynchronous Consensus Zones