Identifying Impacts of Protocol and Internet Development on the Bitcoin Network

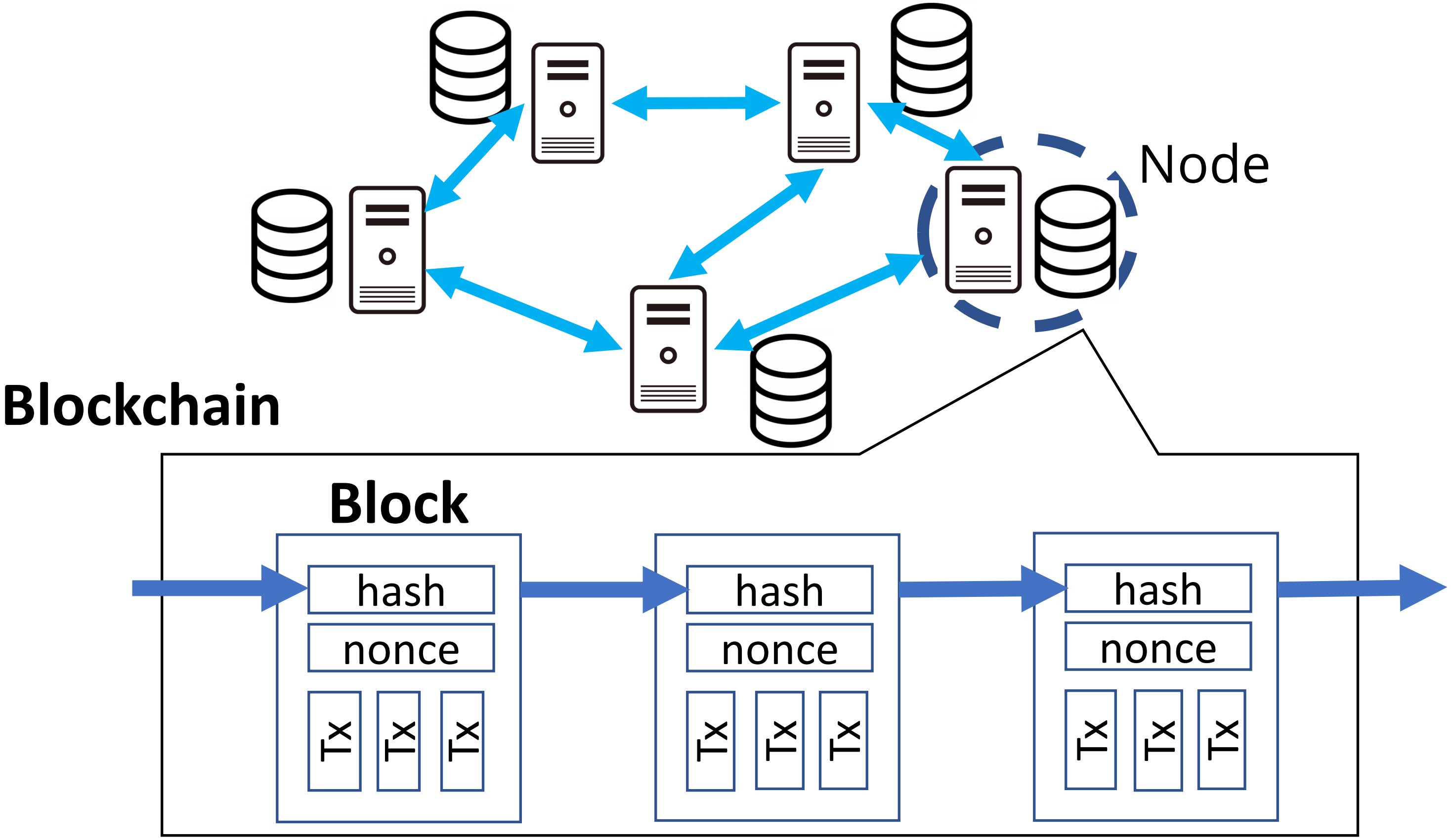
Ryunosuke Nagayama, Ryohei Banno, Kazuyuki Shudo

Tokyo Institute of Technology

Tokyo Tech

Blockchain

- A distributed ledger on P2P network
- A node generates a "block" including transactions and a hash value of its parent block.



Transaction approval

Transaction throughput

Bitcoin: 7 tx/s

$$\frac{\#\ of\ transactions\ in\ a\ block}{Block\ generation\ interval}$$

⇒ **Larger block size**

⇒ **Shorter interval**

Confirmation time

Bitcoin: 10 min × 6 blocks = 1 hour

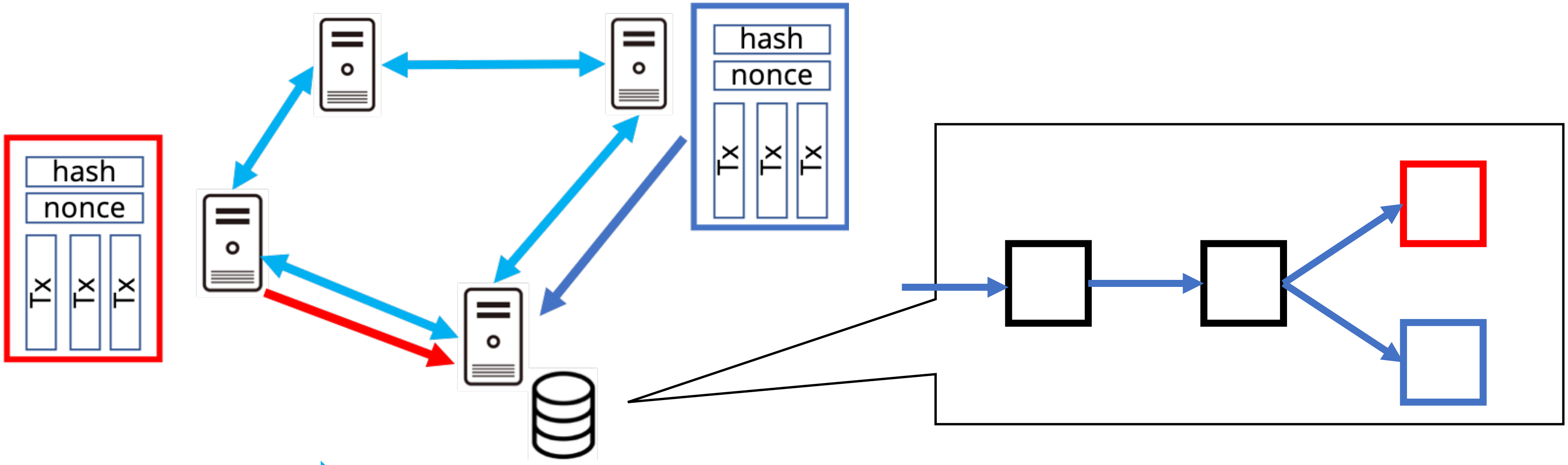
To make overwriting difficult, transactions should be buried under a sufficient number of blocks.

⇒ **Shorter interval**

⇒ **Less number of blocks until confirmation**

Fork

The shorter generation interval and larger block size, the more difficult it becomes to share blocks with other nodes.
If not shared enough, the blockchain will fork and be inconsistent in the network.



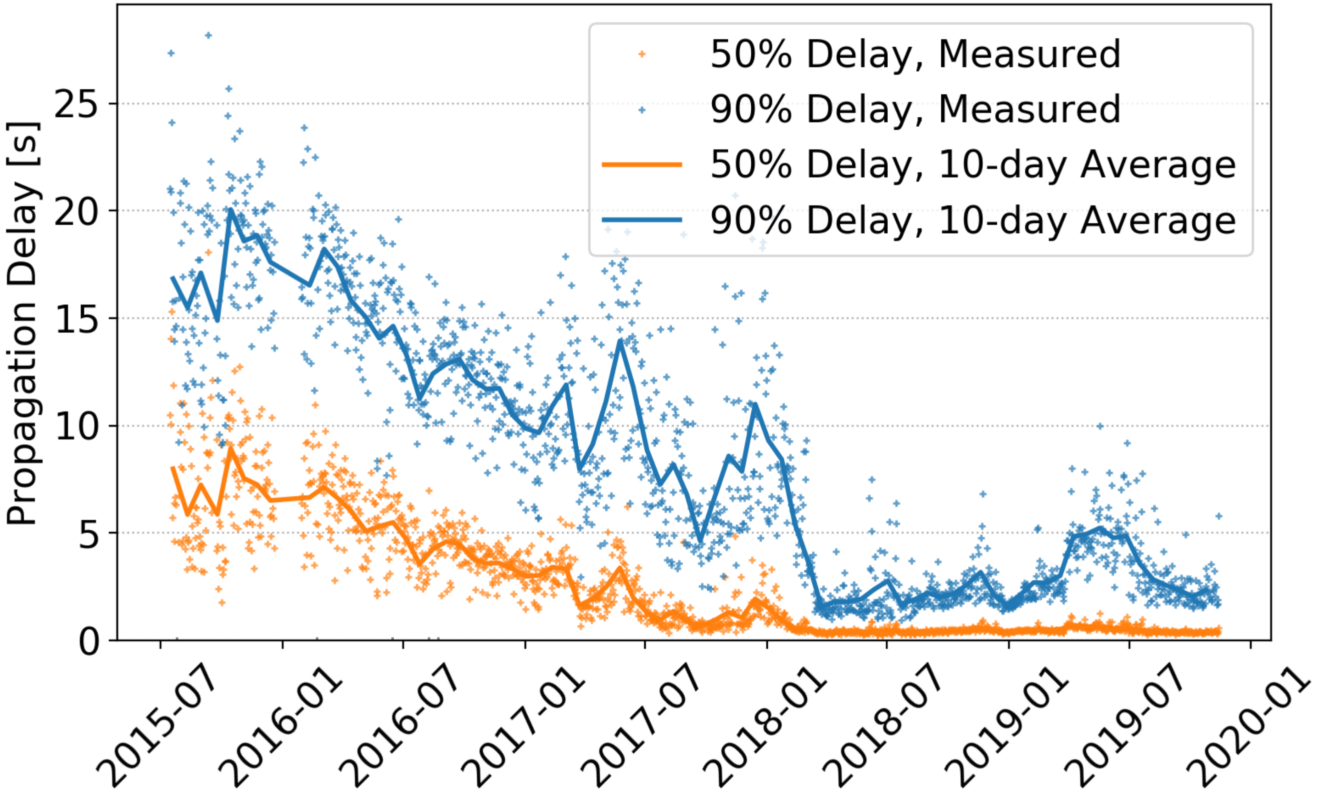
Reduce block propagation delay.

History of block propagation delay on Bitcoin network

Block propagation delay has been reduced

50th percentile ： 8.0 s → **0.4 s**

90th percentile ：16.7 s → **2.3 s**

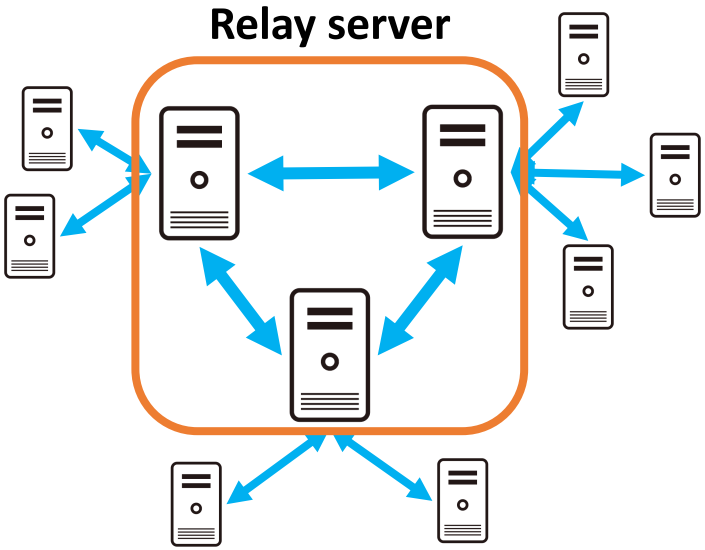


“Bitcoin Network Monitor - DSN Research Group, KASTEL @ KIT,”
https://dsn.tm.kit.edu/bitcoin/

Why has the propagation delay been reduced?

- Relay network

  Relay servers propagate blocks efficiently to participating nodes. [Otsuki, 2019]



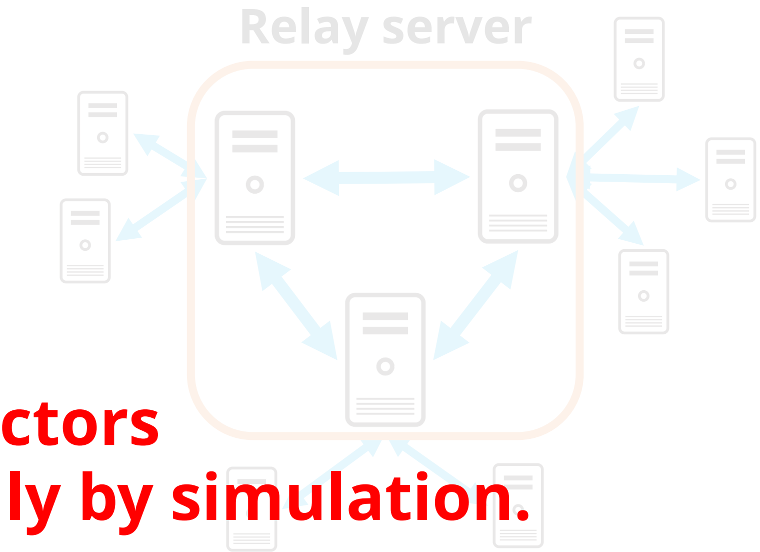
- Development of the Bitcoin protocol
  - Compact block relay (CBR)

- Improvements of the Internet
  - network latency between peers
  - bandwidth

Why was the propagation delay reduced?

- Relay network

  Relay servers propagate blocks efficiently to participating nodes. [Otsuki, 2019]

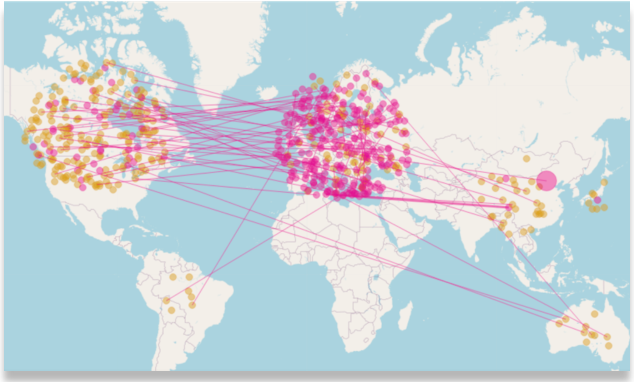


We evaluate following two factors quantitatively and individually by simulation.

- Development of the Bitcoin protocol
  - Compact block relay (CBR)
- Improvements of the Internet
  - network latency between peers
  - bandwidth

Experiment

SimBlock [Aoki, 2019]



A blockchain network simulator that simulates block propagation between nodes. It implements

- Compact Block Relay is implemented.
- Internet parameters as of 2015 and 2019 are implemented.
  - Node distribution

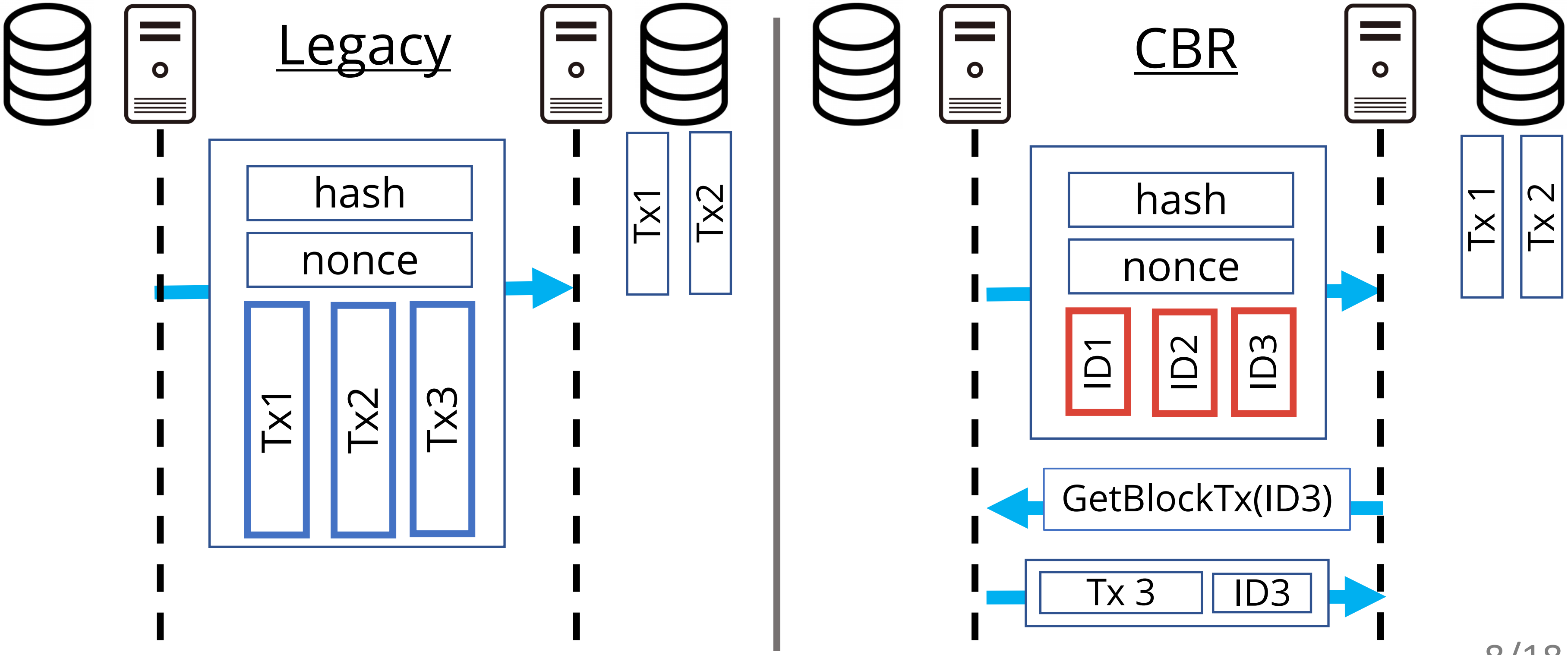
    Number of nodes in each country is obtained from Bitnodes.
  - Network latency

    Weighted average of latency between countries by number of nodes
  - Bandwidth

    Weighted average of bandwidth in countries by number of nodes

Compact Block Relay (CBR)

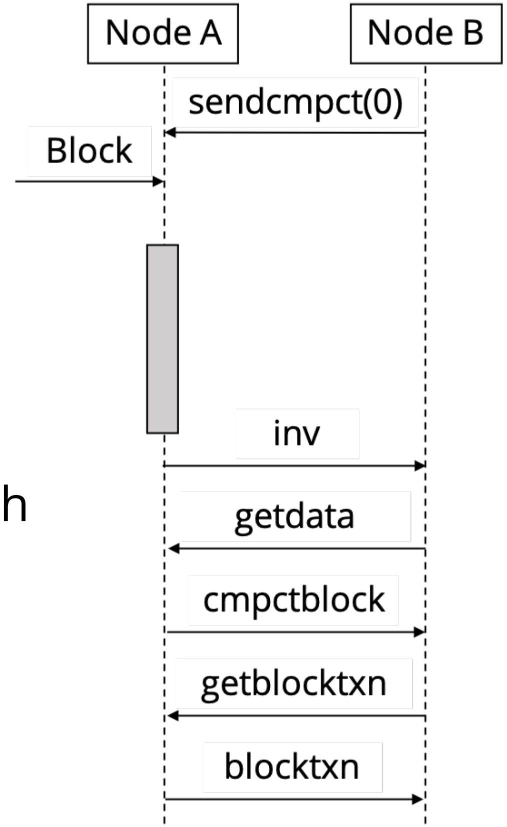
CBR reduces propagation data size by containing only transaction IDs.
If a node does not have transactions approved by a received block (block reconstruct fails), the node request them to its peer.



CBR protocol mode

In high bandwidth relaying, nodes send compact block before block validation, and do not send inv message. It wastes bandwidth.

→ We assume nodes use low bandwidth relaying.



Node A

Node B

sendcmpct(0)

Block

inv

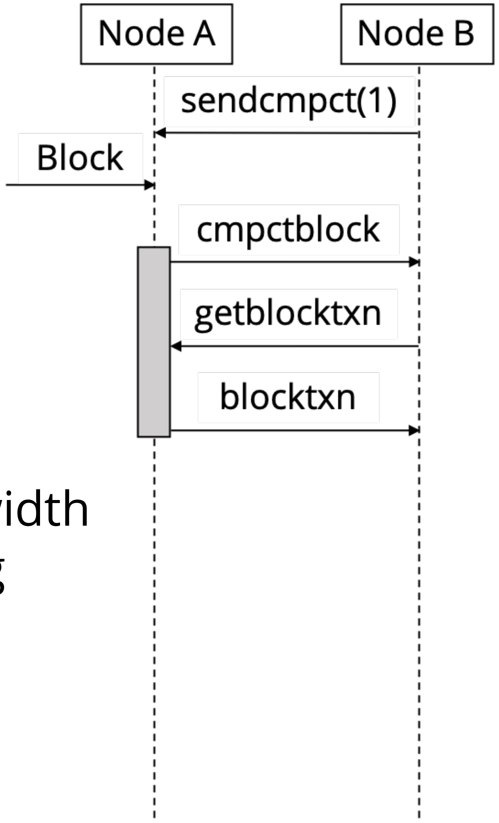
getdata

cmpctblock

getblocktxn

blocktxn

Low Bandwidth Relaying



Node A

Node B

sendcmpct(1)

Block

cmpctblock

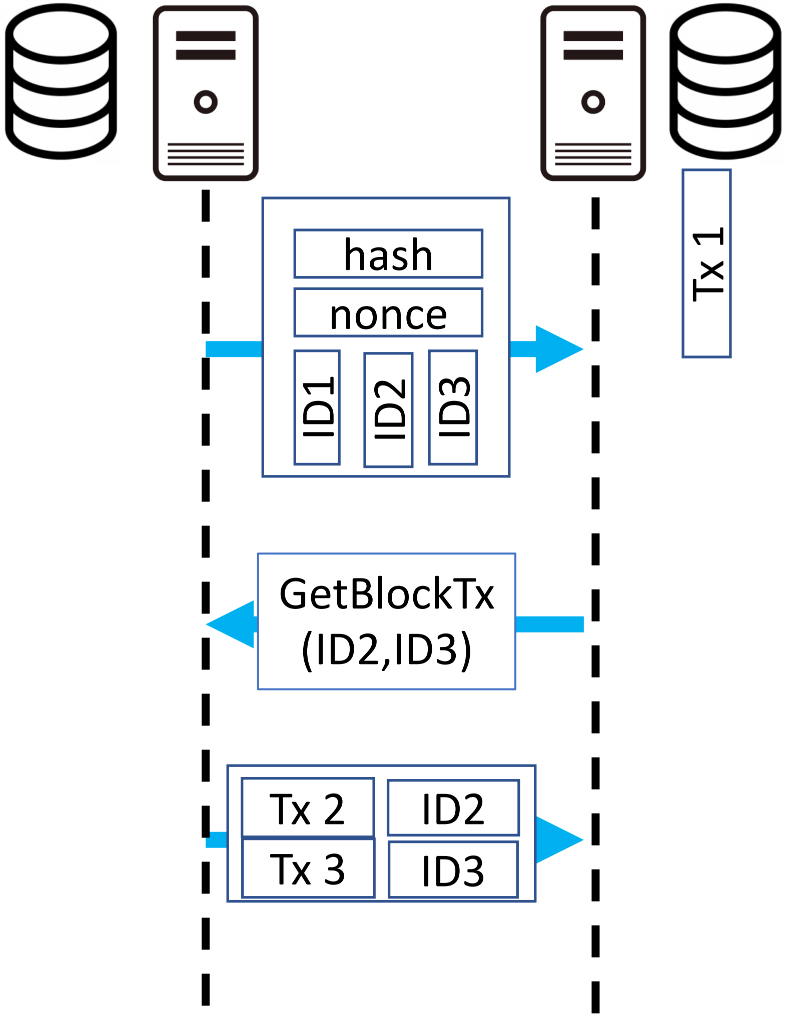
getblocktxn

blocktxn

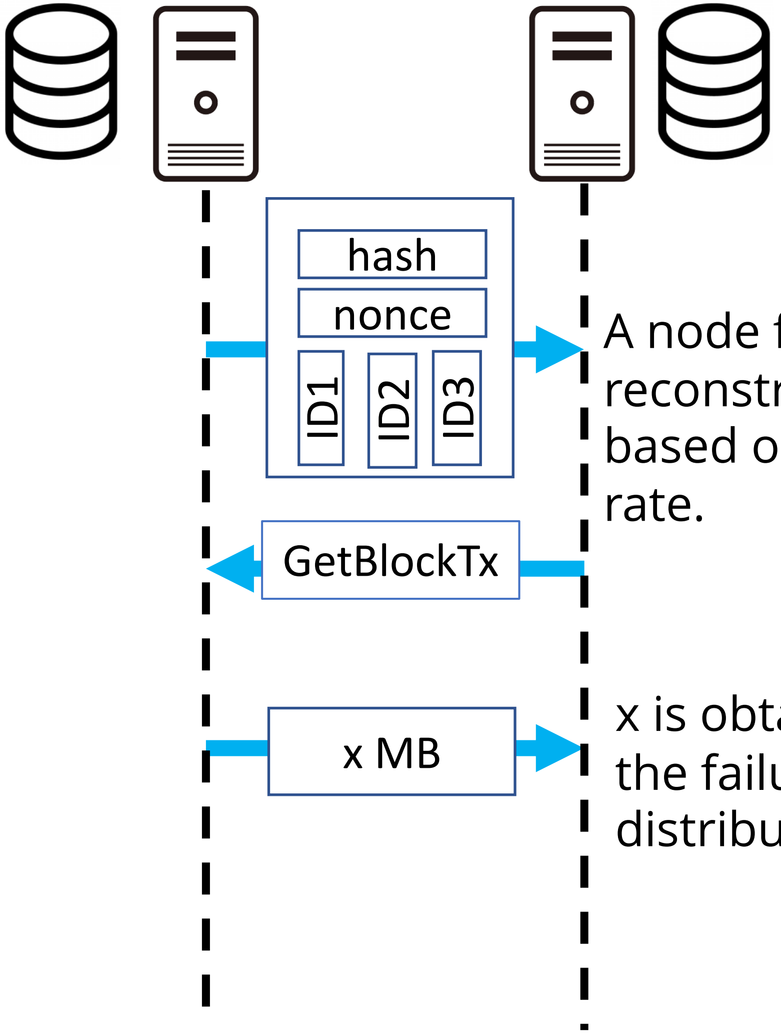
High Bandwidth Relaying

Modeling block reconstruct failure

Actual CBR



Our approximate model



A node fails reconstruct based on failure rate.

x is obtain from the failure size distribution.

CBR Parameters

- Compact block size 18 KB[Ozisik 2016]

- CBR usage rate 96.4 %
    - The usage rate is based on the versions of protocol used by each nodes obtained from Bitnodes.

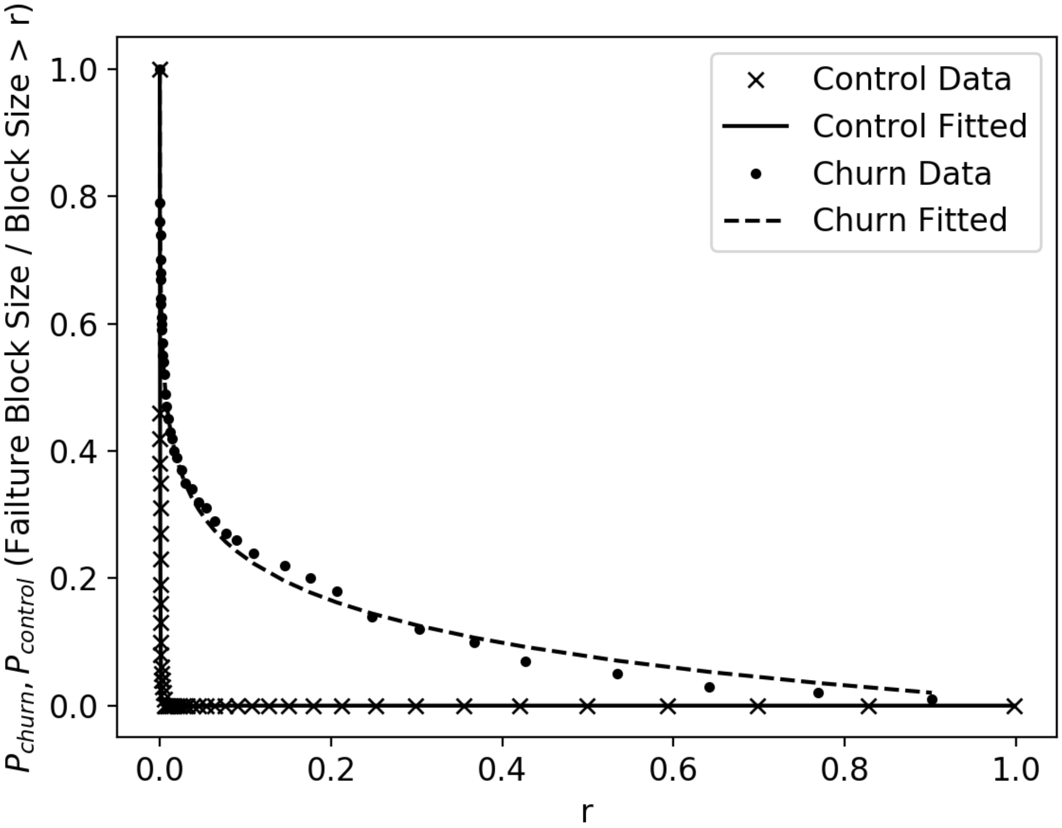
- Reconstruction failure rate
    - Imtiaz et. al[Imtiaz 2019] measured
    - Churn node 27 %
    - Control node (Stay connected to the network) 13 %

- Ratio of churn nodes 97.6%
    - Imtiaz et. al[Imtiaz 2019] measured

[Ozisik 2016] A. P. Ozisik et. al, "A secure efficient and transparent network architecture for Bitcoin", 2016.
[Imtiaz 2019]Muhammad Anas Imtiaz et. al, Churn in the Bitcoin Network: Characterization and Impact, IEEE International Conference on Blockchain and Cryptocurrency, 2019

Data size received from peer when reconstruction fails

The data size is obtained from the cumulative distribution that approximates the data measured by Imtiaz et. al[Imtiaz 2019].



[Imtiaz 2019] Muhammad Anas Imtiaz et. al, Churn in the Bitcoin Network: Characterization and Impact, IEEE International Conference on Blockchain and Cryptocurrency, 2019

Comparison with measured data

		Measured[2]	Our simulation
50%ile	2015	7,988 ms	9,673 ms
	2019	401 ms	1,304 ms
90%ile	2015	16,835 ms	14,056 ms
	2019	2,353 ms	2,364 ms

Simulated values are comparable with measured values except to 50th percentile of 2019.

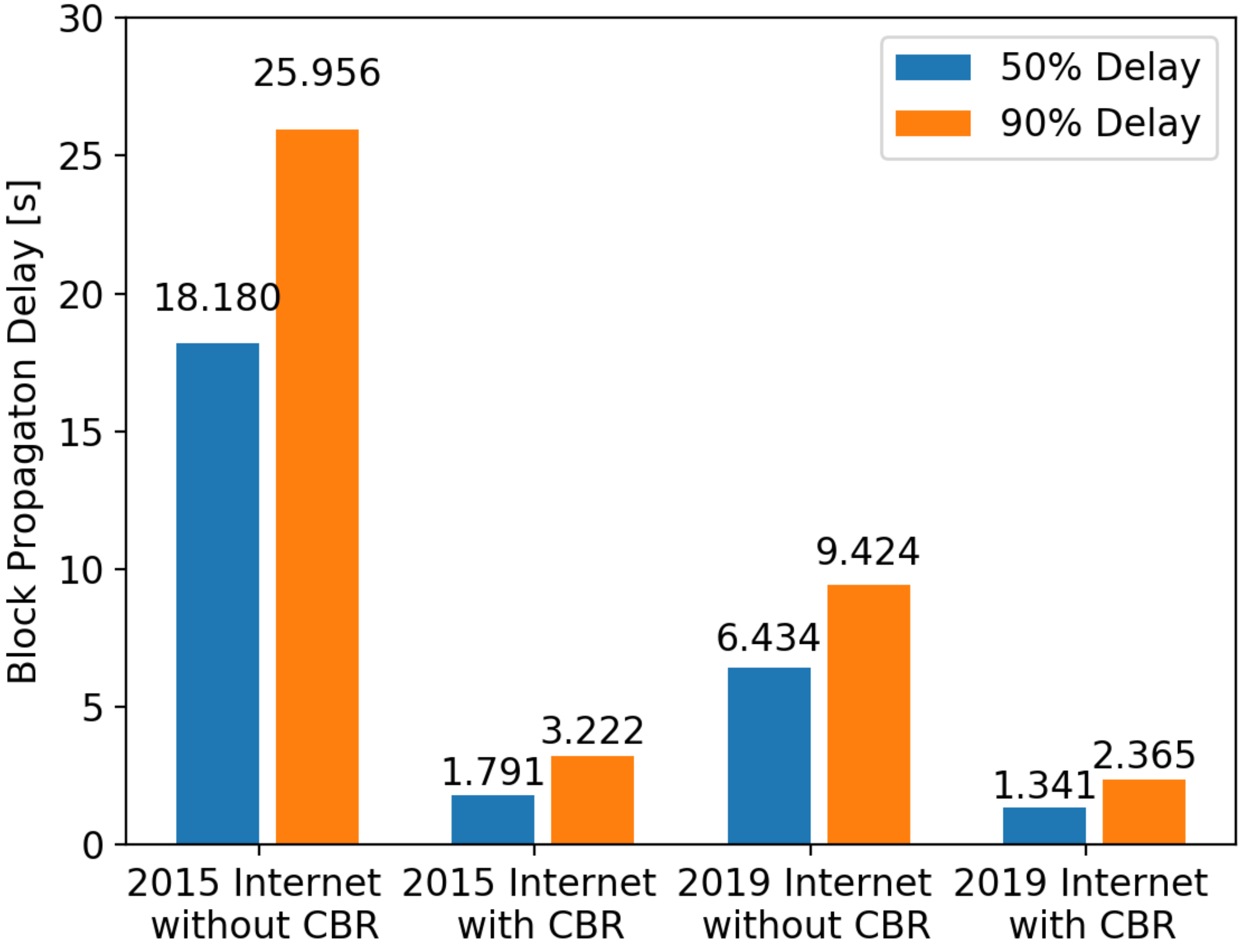
→ **Relay network**

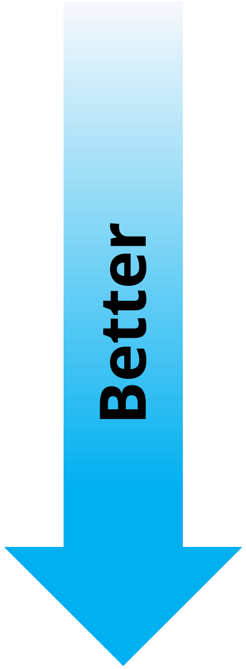
Our simulation assumes a random network without a relay network.
Relay network efficiently propagates to participating nodes
Participation rate 2.65 %[4]

[2] “Bitcoin Network Monitor - DSN Research Group, KASTEL @ KIT,” https://dsn.tm.kit.edu/bitcoin/

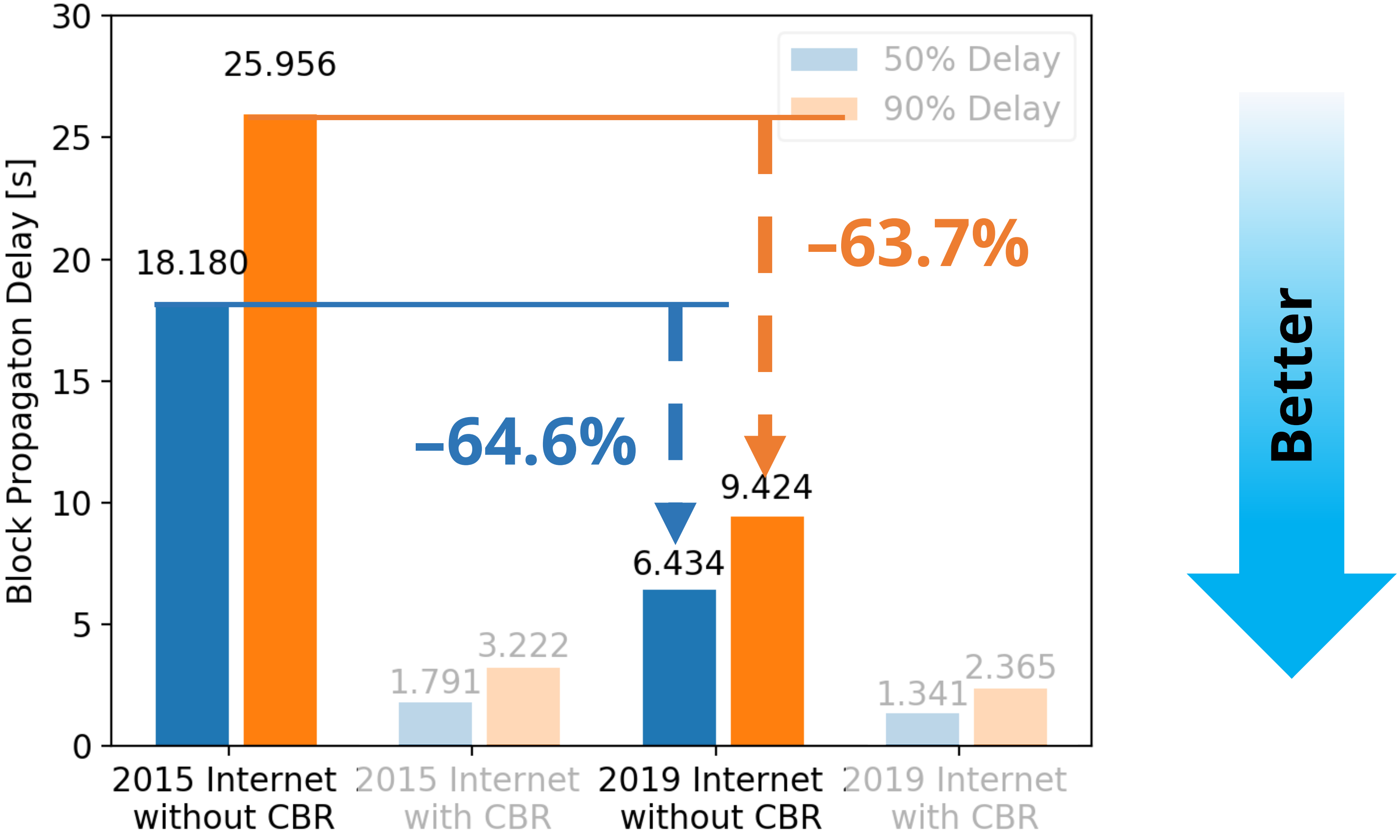
[4] “Falcon - a fast bitcoin backbone,” https://www.falcon-net.org/

Identifying impacts of CBR and Internet improvement on the Bitcoin Network

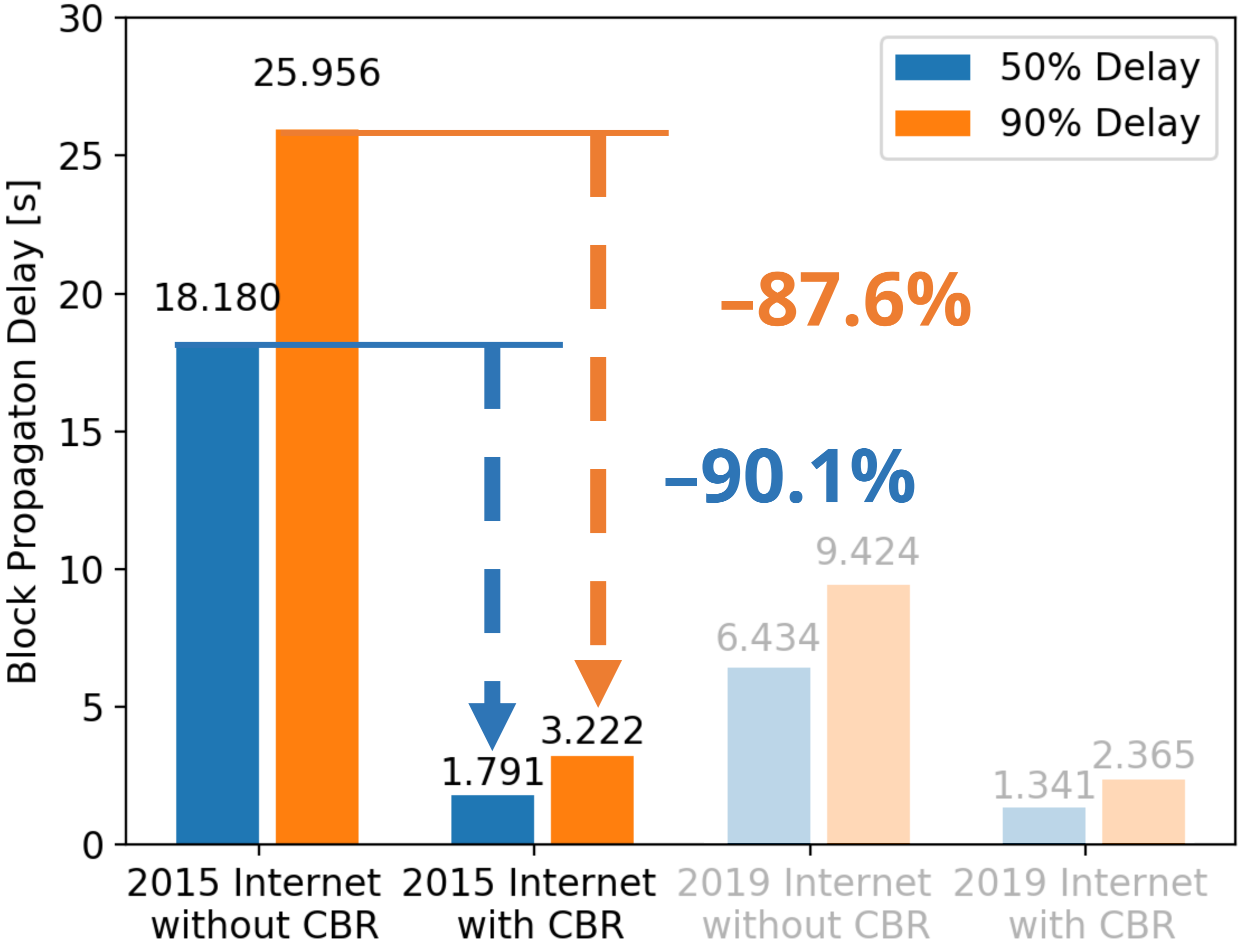


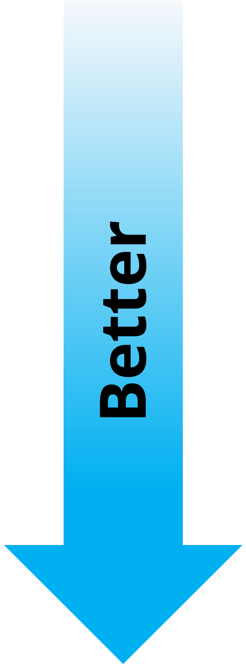


Internet 2015 vs 2019

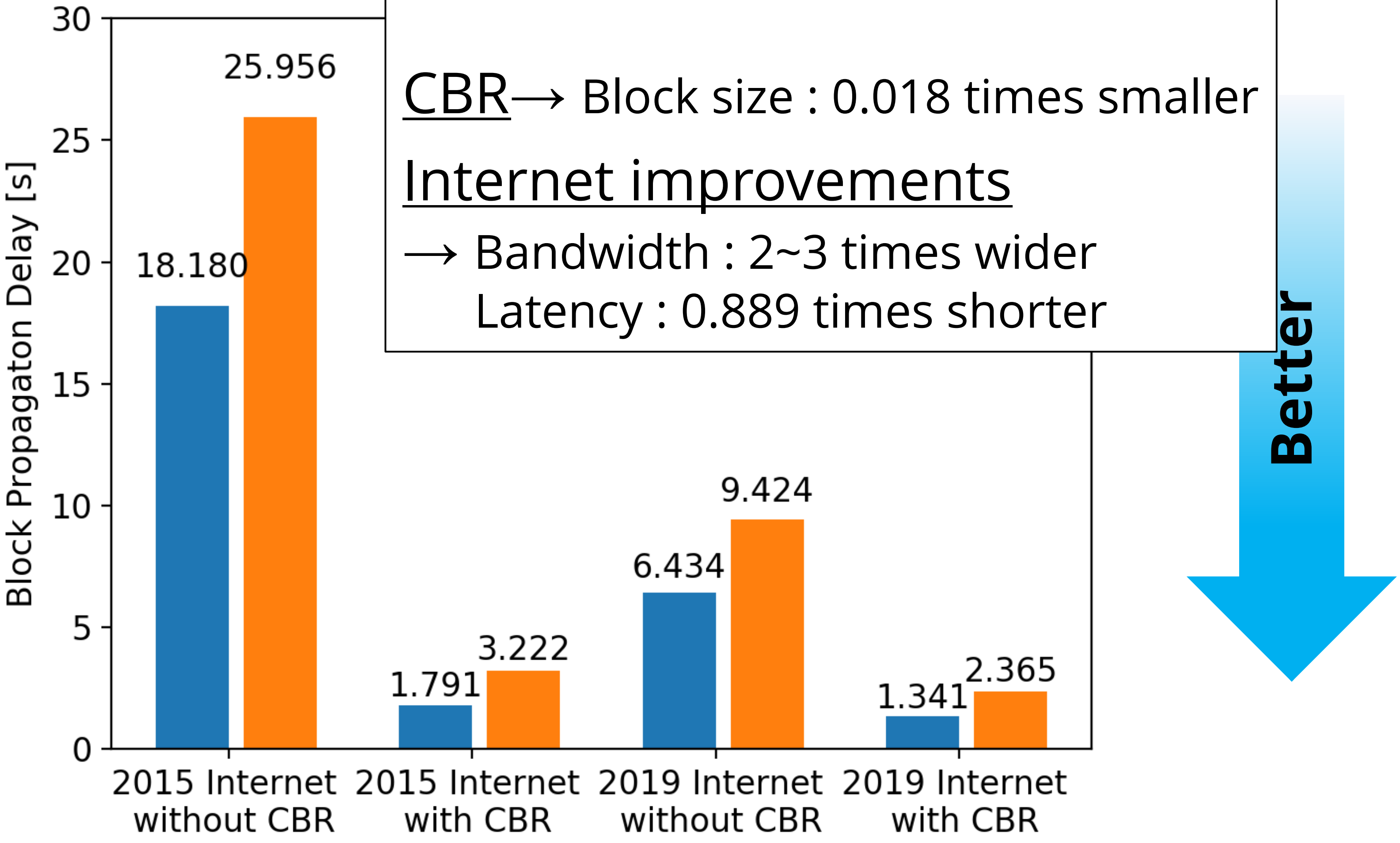


With CBR vs without CBR





Block propagation delay



CBR was more effective.

CBR→ Block size : 0.018 times smaller

Internet improvements

→ Bandwidth : 2~3 times wider
Latency : 0.889 times shorter

Conclusion

- CBR significantly improved the propagation delay.

- Since CBR can be applied to other blockchains, it can be expected that CBR shortens the propagation delay in other blockchains.