French-Japanese workshop
on blockchain technologies and applications to digital trust
November 14th and 15th, 2023

bit.ly/shudo20231114

Tradeoffs Inherent in Blockchain

Kazuyuki Shudo
Kyoto University
首藤 一幸
京都大学

SimBlock

Kyoto U. Tokyo Tech

Kazuyuki Shudo (49)

1996 Master course, Waseda U.
1998 Ph.D. course, Waseda U.
2001 AIST **National laboratory**
2006 Utagoe, Inc. **Startup**
2008/12 Tokyo Tech **University**
2022/ 4 Kyoto University
2009/ 5 Project manager of Mitou program
2023/ 4 Project manager of Mitou Adv. program

2018/11 Advisor, Earlyworks Co., Ltd.
2019/ 1 Mentor, Miraise1 LLP
2022/ 7 Technology Advisor, GMO Internet Group, Inc.
2022/10 Advisor, GMO AI & Web3 Inc.
2023/ 6 Director, Information Processing Society of Japan

Java thread migration system MOBA
Java Just-in-Time compiler shuJIT
17,000 downloads, commercial uses
P2P middleware Overlay Weaver
26,000 downloads from 15 countries
Database w/ 673 servers in 41 countries
P2P live streaming UG Live
2 Mitou supercreators, commercialized, simultaneous 10,000 or more audiences
A book Binary Hacks
5 authors, over 10,000 sold
P2P algorithms, 2009 ~
A universal framework for structured overlay / DHT
Distributed databases, 2009 ~
High perf. in both read & write, Causal consistency, NVRAM/SCM
Simulation of distributed systems, 2011 ~
100M nodes / 10 servers, 20X perf., on Apache Spark
Social network analysis, 2013 ~
Decentralized distributed ML, 2016 ~
Blockchain, 2016 ~
A simulator SimBlock, Perf. & security, new architecture

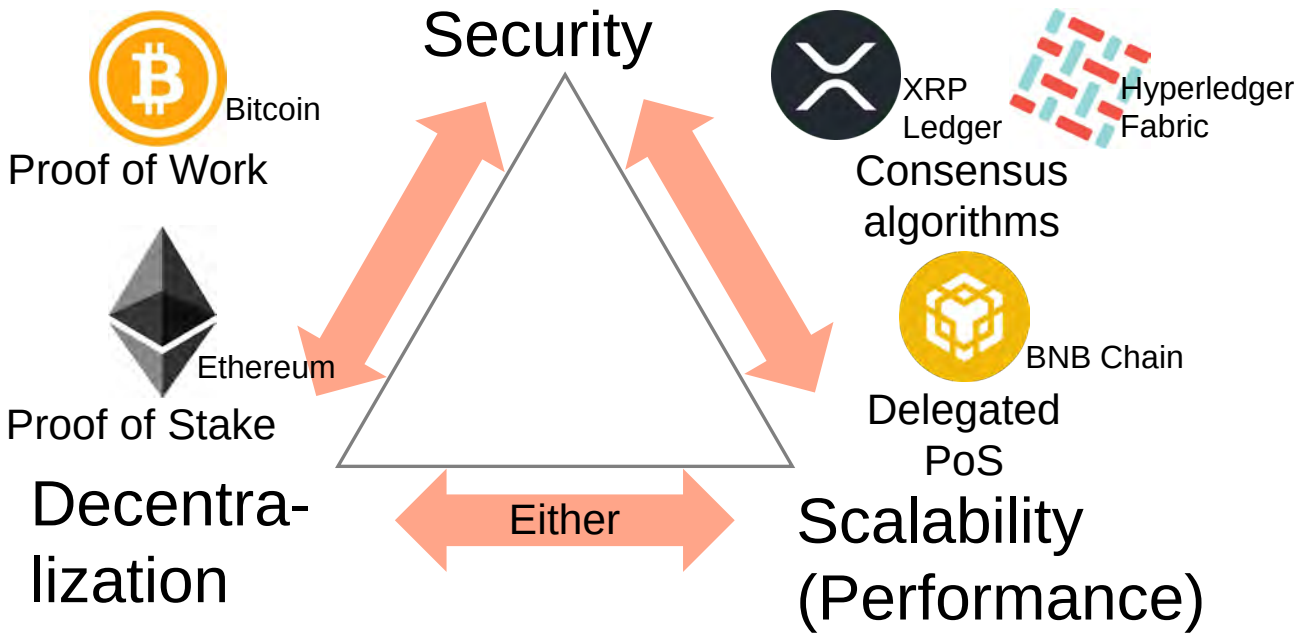
As of Nov. 2023

Software like a magic

Large-scale distributed systems

The blockchain trilemma

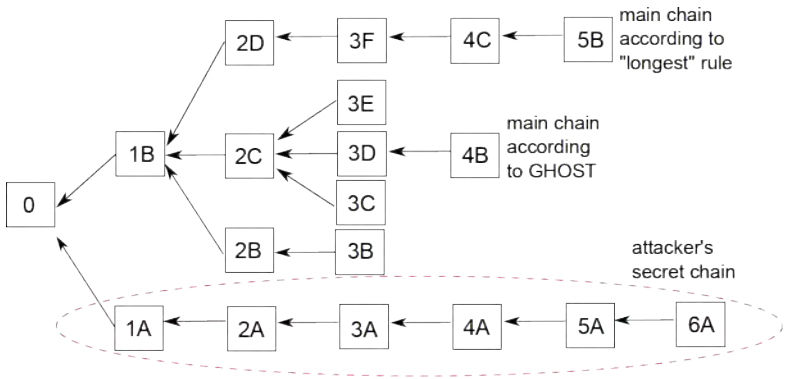
- Termed by Vitalik Buterin, a founder of Ethereum, in 2017



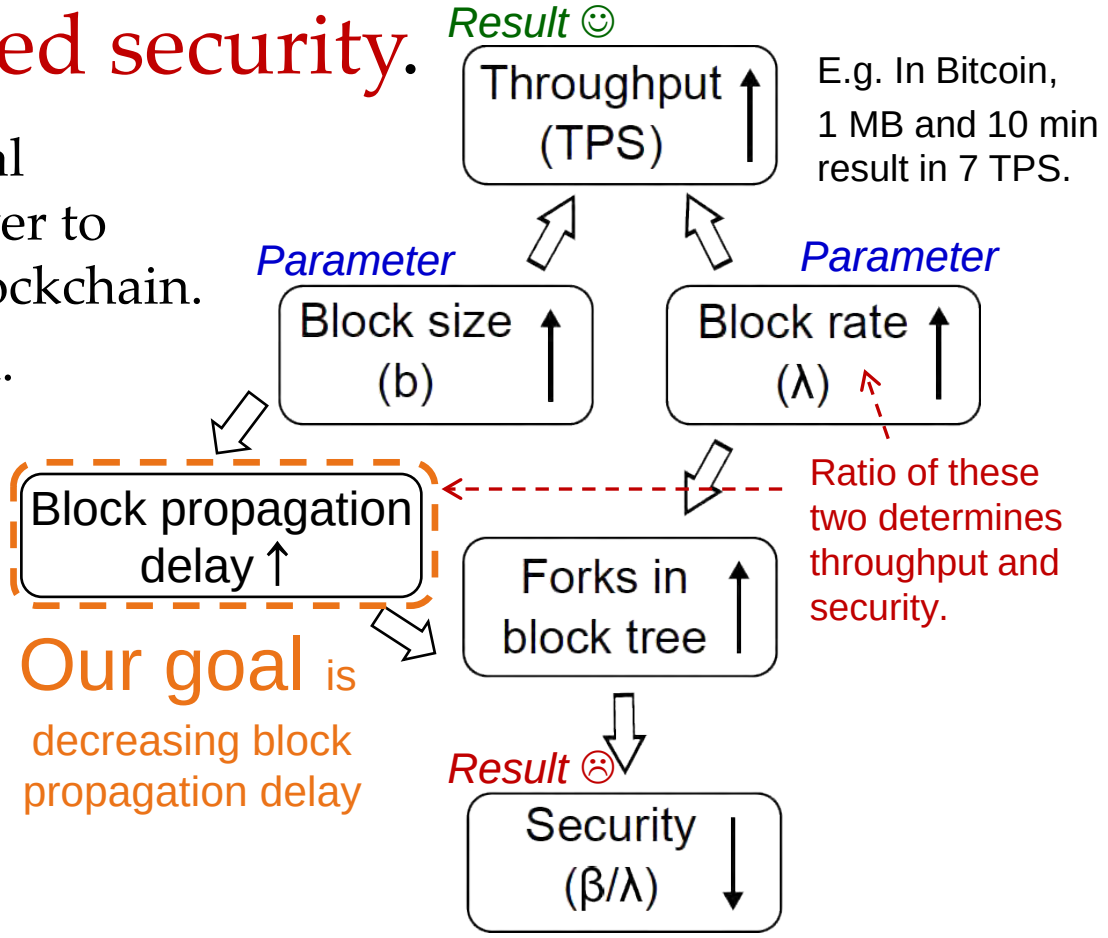
- We all roughly recognize it.
  - Detailed discussion: What is decentralization? …

A tradeoff between performance and security

- Naïve throughput improvement techniques result in decreased security.
  - Forks disperse the total confirming (hash) power to multiple tails of the blockchain.
  - It facilitates 51% attack.



An example of highly forked blockchain.

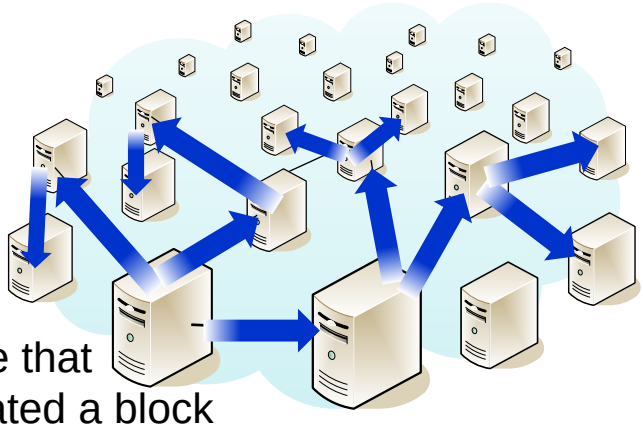


Figures are from “Secure High-Rate Transaction Processing in Bitcoin”, FC’15, 2015

Blockchain "network" matters

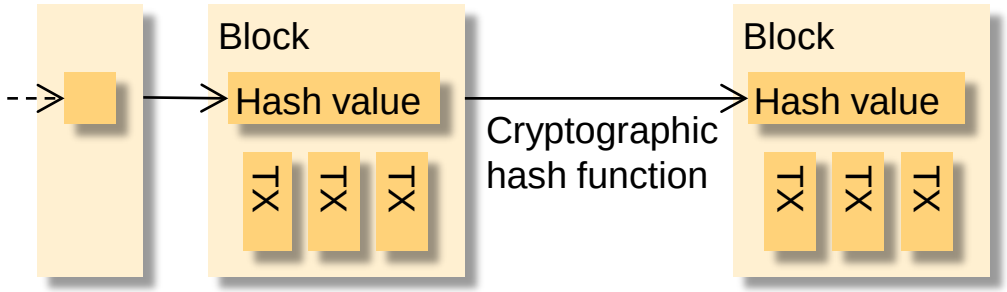
- Performance: # of transactions (TX) / second = TPS
  - An example of a TX: Transfer of 1 BTC from Alice to Bob
  - Existing payments VISA: thousands TPS, PayPal: 320 TPS in average
  - Cryptocurrency Bitcoin: 7 → 27 TPS, Ethereum: around 15 TPS …insufficient
- Perf. improvements requires faster block propagation.

See the last slide.



A node that generated a block

A network of nodes (servers)



Data structure of a blockchain

A block is propagated between nodes and broadcasted to all the nodes.

Table of contents

- Tradeoffs
  - The blockchain **trilemma**
  - **Tradeoff** between performance and security

Hypothetical
[Buterin 2017]

- Research results in our group
  - Tool
  - Scalability (performance)
  - Security

Well-grounded
[Sompolinsky 2015]

- The blockchain **trilemma** described by a formula

Well-grounded
[IEEE Blockchain 2023]

Our results

- Topics expand from **tool** and **performance** to **security** and **trustless**.

Security

Tolerance for selfish mining [Devcon 5a]

Impacts of a countermeasure to Erebus attack [IEEE Access 2021]

An attack to PoS and tolerance examination [IEEE ICCE 2023]

Theoretical fork rate

Influence mutually

Performance

Estimating block propagation time [AINTEC 2019]

Neighbor selection [IEEE Blockchain 2019]

Impacts of CBR and Internet improvements [IEEE ISCC 2020]

Impacts of relay networks [IEEE Blockchain 2020]

Broadcast tree [Kitagawa 2023]

Block sender switchover [IEEE ISCC 2023b]

Notification of block generation [IEEE ISCC 2023a]

Block interval adjustment [IEEE Blockchain 2022b]

Provide a research tool

Tool

Simulator SimBlock [CryBlock 2019] [IEEE ICBC 2019] [Devcon 5b] [IEEE ICBC 2023]

Incentive mismatch problem

Application migration between chains [IEEE HotICN 2018]

Trustless

Eval. of (de)centralization [IEICE SIG-NS 2019]

A compact data structure [IEICE trans. 2022]

UTXO aggregation [IEEE Blockchain 2022c]

Clock synchronization [IEEE Blockchain 2022a]

A fairness index and its improvement [BlockDM 2020]

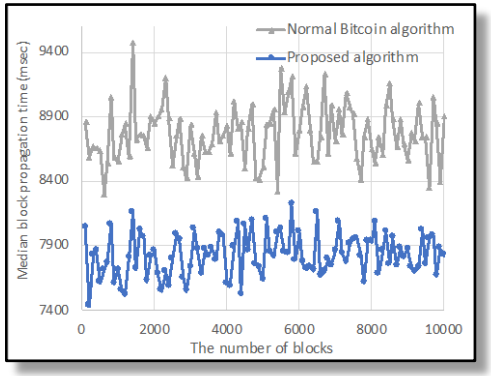
Provide a research tool

A talk in Devcon 5 [Devcon 5a]
(An Ethereum developer's conference)

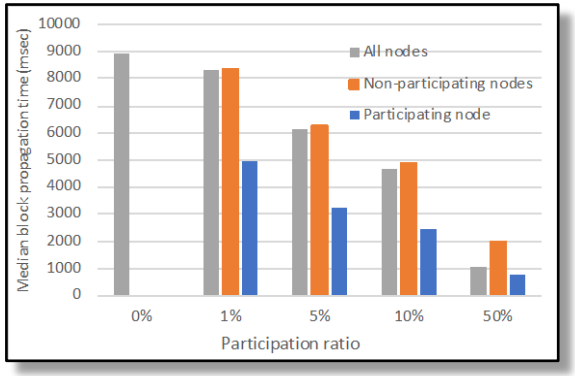
Simulator SimBlock

[CryBlock 2019] [IEEE ICBC 2019] [Devcon 5b] [IEEE ICBC 2023]

- A public blockchain "network" simulator
  - developed at Tokyo Tech, and released in June 2019.
- It simulates transmission of blocks
  - Bandwidth and latency over Internet as of 2015 and 2019
    - Intra/inter region BW and latency of 6 regions on the earth
  - Behavior of nodes: Block generation interval, transmission, Compact Block Relay
    - Parameters of Bitcoin, Litecoin and Dogecoin
- Visualizer provided
- Researches :



Neighbor selection
[IEEE Blockchain 2019]

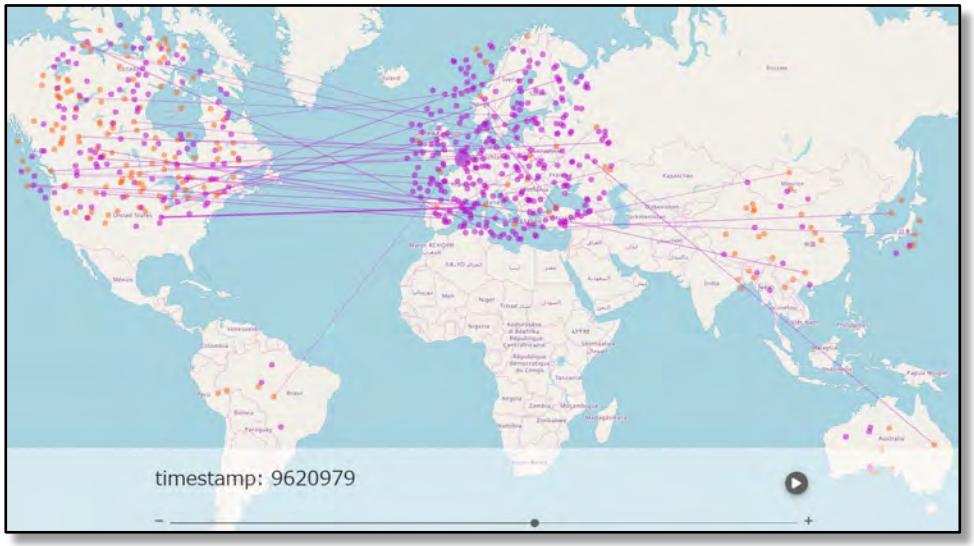


Impacts of relay networks
[IEEE Blockchain 2020]

Results: Tool

Simulator SimBlock

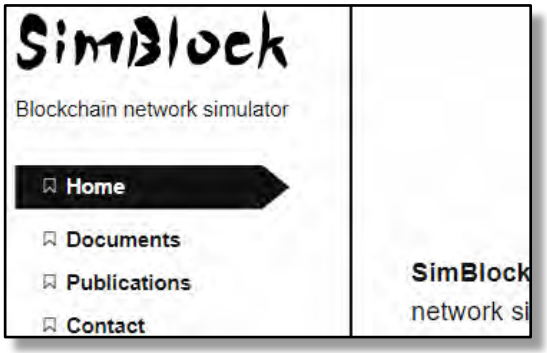
[CryBlock 2019] [IEEE ICBC 2019] [Devcon 5b] [IEEE ICBC 2023]



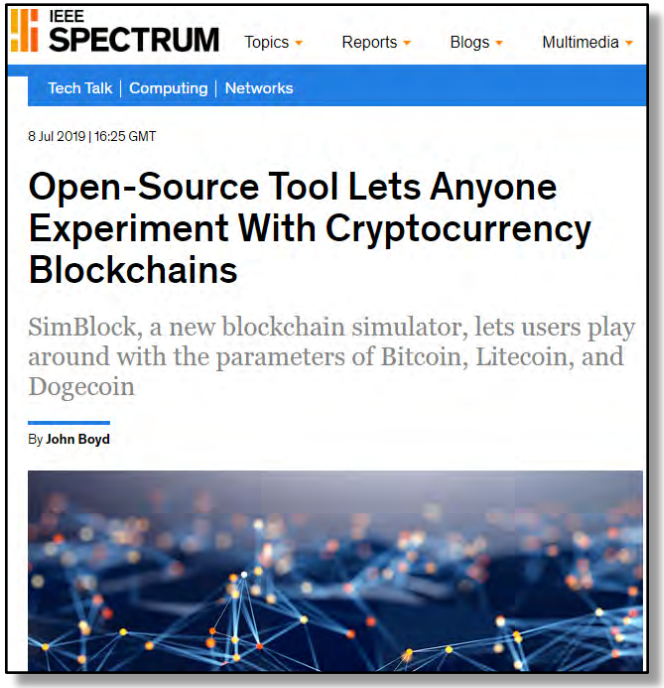
Visualizer Bitcoin network,
scaled down to 600 nodes for demo

Demo
at IEEE ICBC 2019
in Seoul, and
at IEEE ICBC 2023
in Dubai

Web site

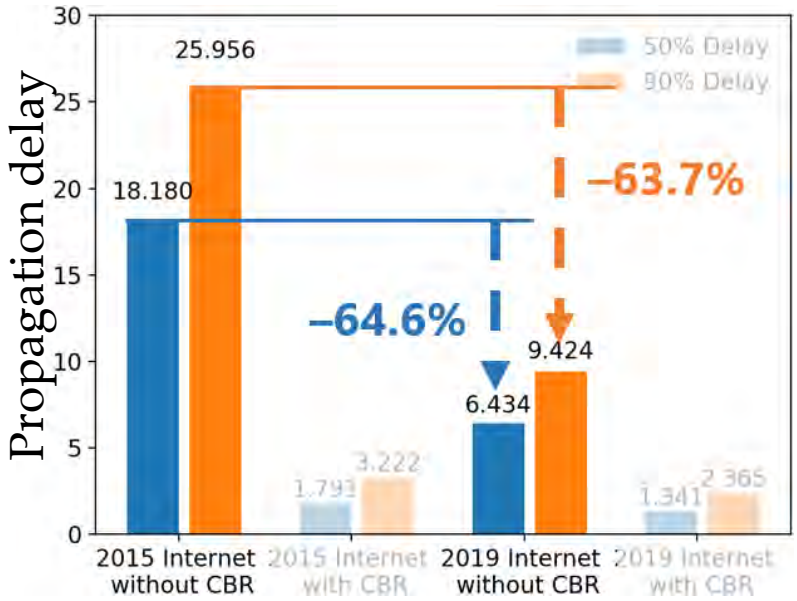


Article on
IEEE Spectrum



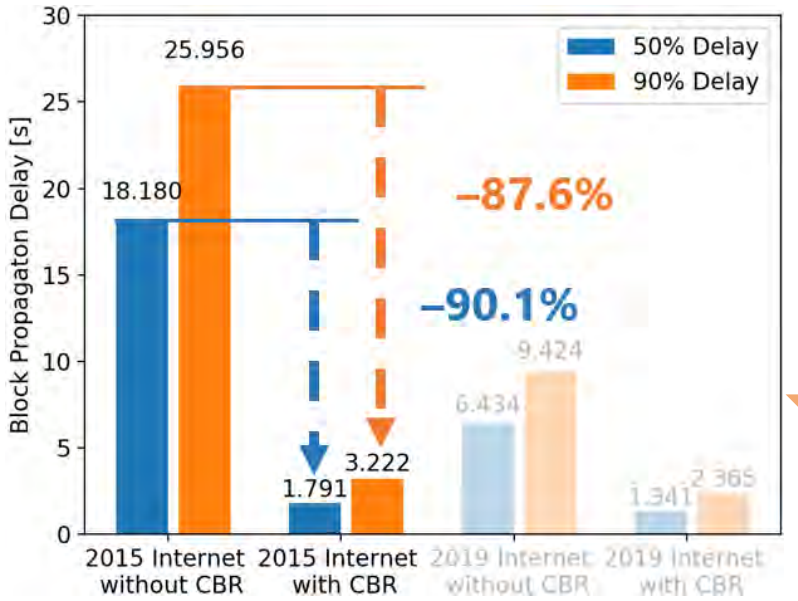
Impacts of Internet improvements and Compact Block Relay [IEEE ISCC 2020]

- SimBlock enabled comparisons:
  - Internet as of 2015 and 2019
  - Presence or absence of Compact Block Relay
    - Block propagation protocol implemented in Bitcoin 0.130 in Aug. 2016



Impact of Internet improvements from 2015 to 2019

<

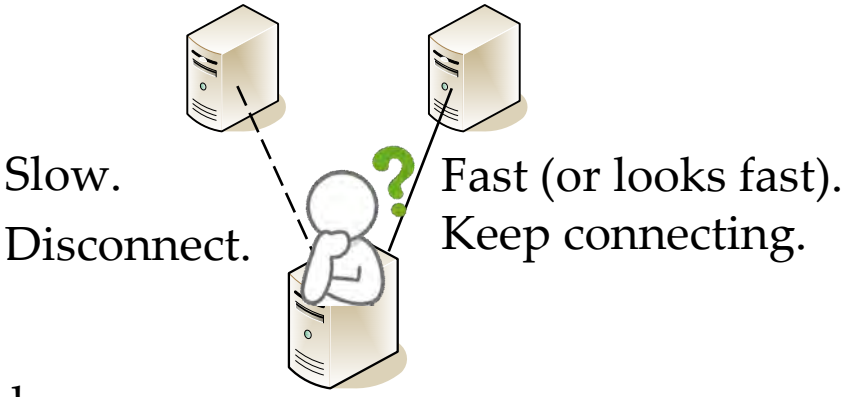


Impact of Compact Block Relay

Proximity Neighbor Selection

[IEEE Blockchain 2019]

- Selecting a neighbor node based on communication performance
  - A major technique in peer-to-peer field
    - We tried it for DHTs [IEEE ISCC'13]
- Simulator SimBlock was developed for this study

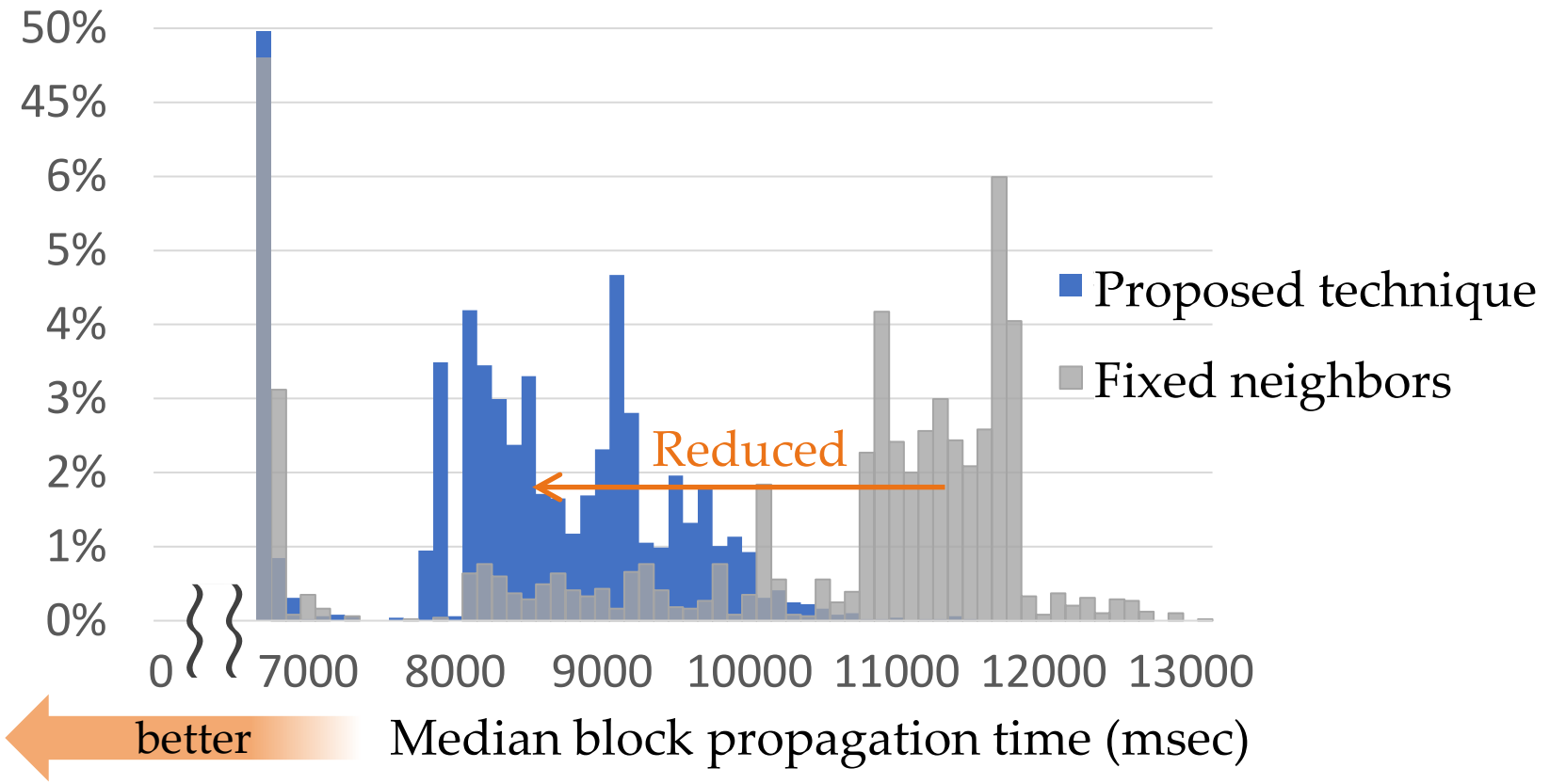


- Procedure
  - Scoring all the nodes that gave me a block
    - Score = exponentially weighted average of (Block arrival time – generation time)
  - Re-selecting neighbor nodes per 10 blocks received
    - However, selecting K nodes randomly to connect new nodes
    - The best parameter: K = 1, P (weight of the newest propagation time) = 0.3

Proximity Neighbor Selection

[IEEE Blockchain 2019]

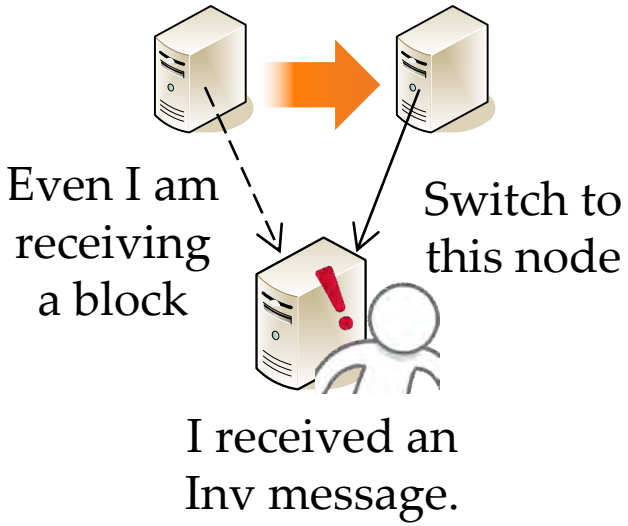
- Reduced from 11.5 sec to 8.5 sec
  for slowly propagated blocks.

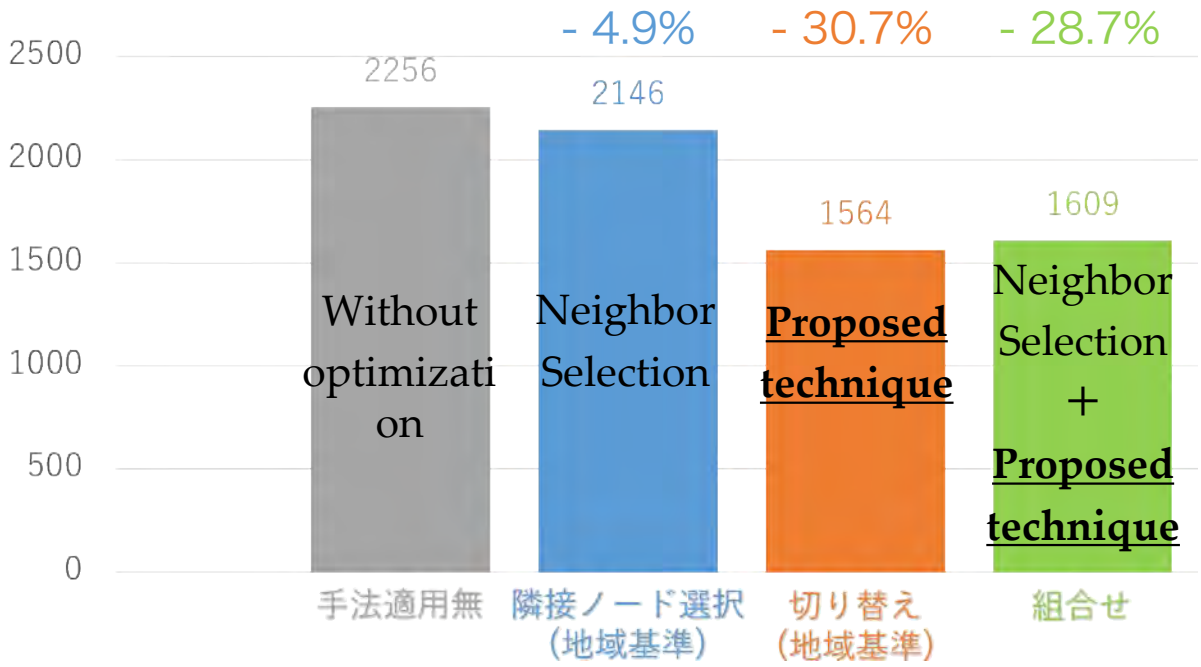


Block sender switchover

[IEEE ISCC 2023b]

- A node switches the block sending node even if it is receiving a block.
  - A node receives data that it has already received. Though, performance is improved. Note that a protocol extension eliminates such wasteful comm.



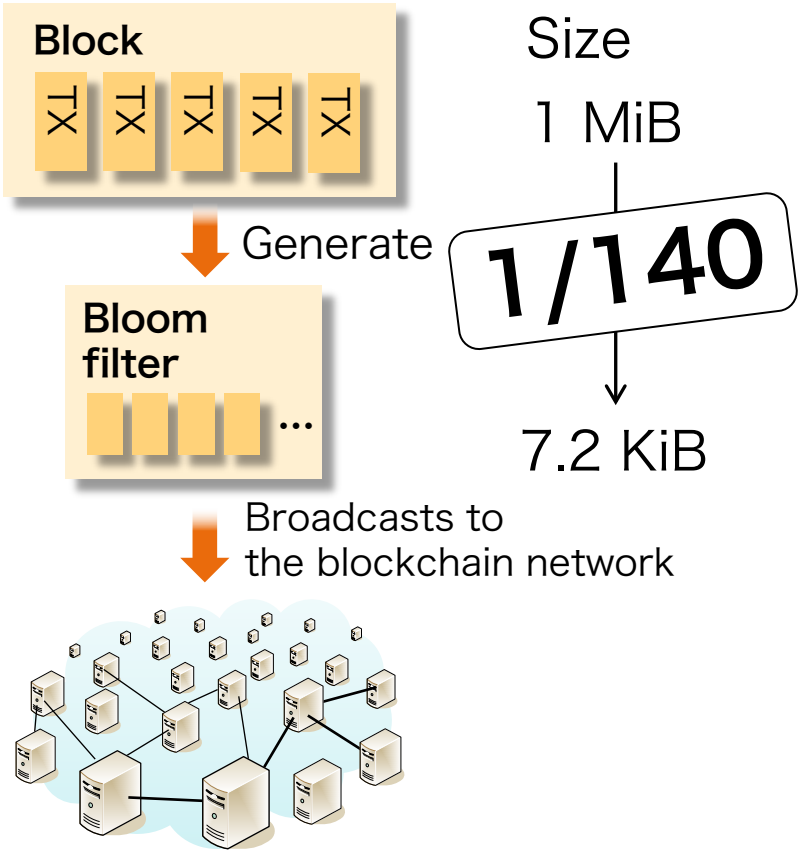


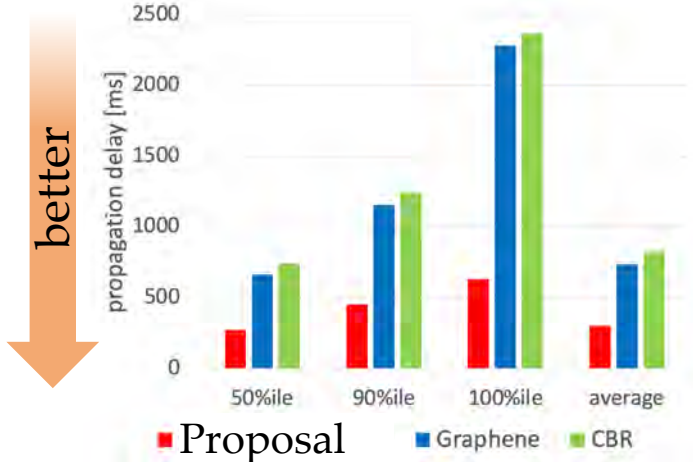
Block propagation time to 90% of nodes

Quick notification of block generation

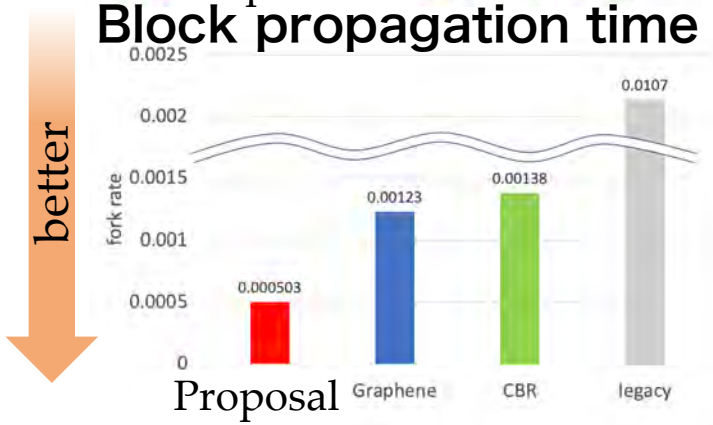
[IEEE ISCC 2023a]

- Broadcasting a bloom filter before the block.
  - The bloom filter summarizes the block.





Block propagation time

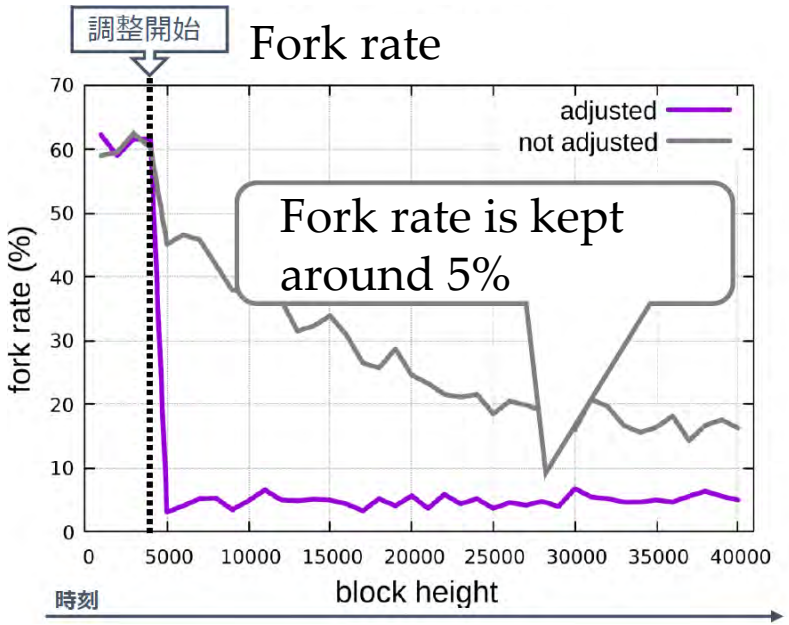


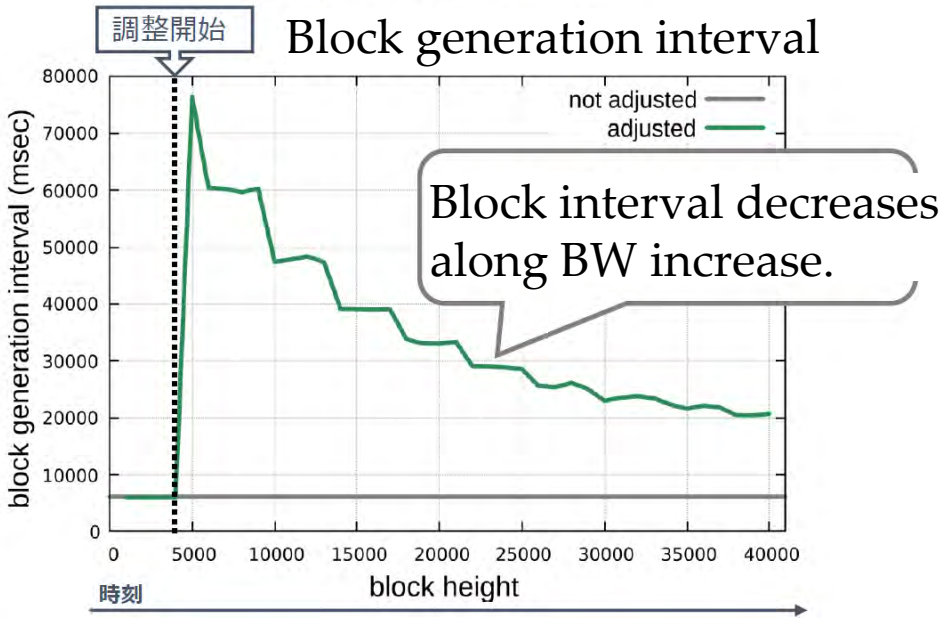
Fork rate (a security index)

Dynamic adjustment of block generation interval

[IEEE Blockchain 2022b]

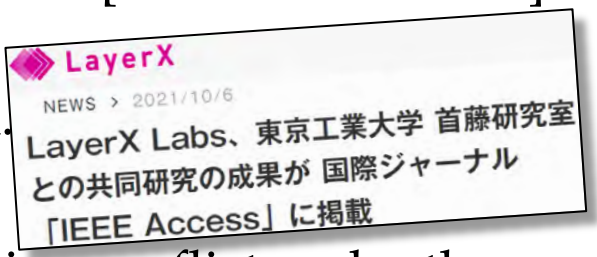
- Performance (TPS) = # of TX in a block / block interval
  - Bitcoin in 2009: 7 TPS = 1 MiB / 250 byte / 600 second
- Proposal: Adjusting block interval while keeping security
  - Not sacrificing security = keeping the fork rate constant
  - Estimating the fork rate based on block arrival times at nodes



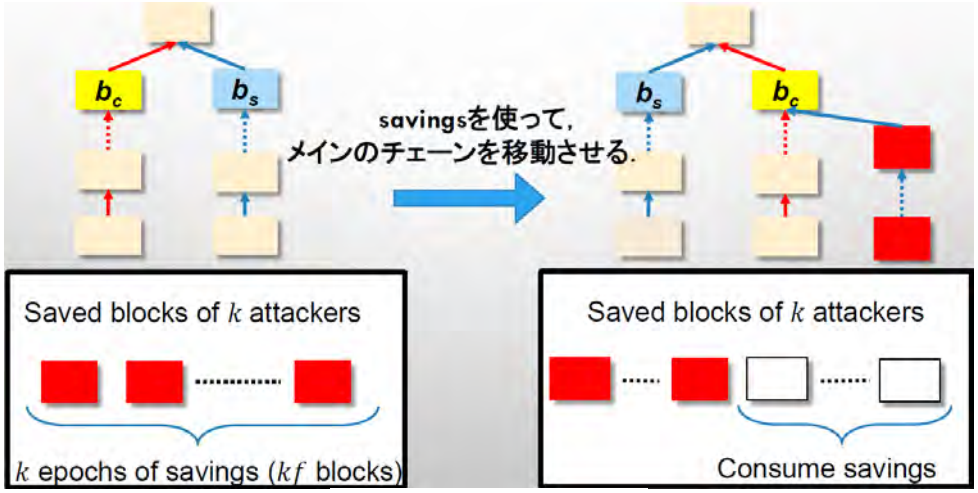


Saving attack to Ethereum-style PoS blockchains and tolerance evaluation

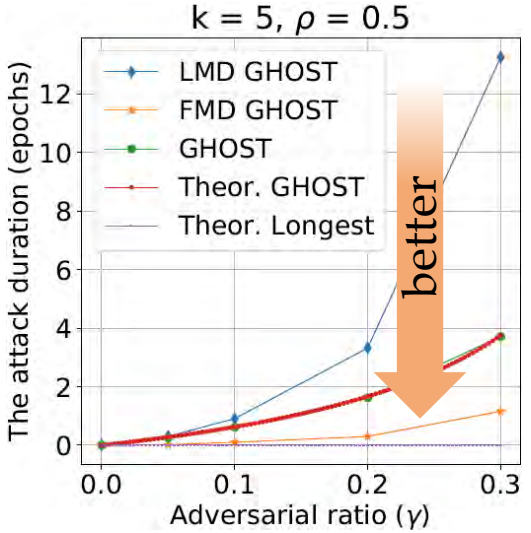
[IEEE Access 2021]



- A saving attack discovered
  - An adversary saves the right to block generation.
  - It generates a block at the most convenient time.
  - It keeps a vulnerable condition in which two chains conflict each other.
- We evaluated tolerance for the attack, of each fork choice rule
  - FMD GHOST is the best, as planned



Saving attack



LMD GHOST

GHOST

FMD GHOST

Accurate expression of theoretical fork rate

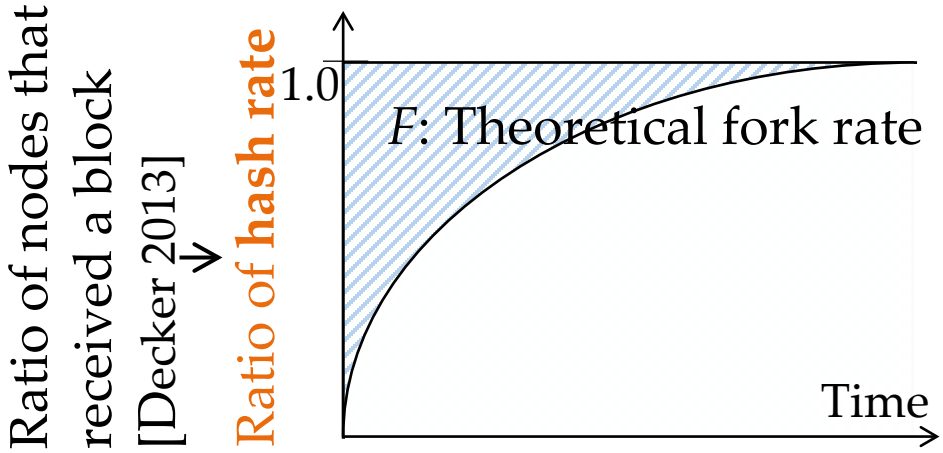
[IEEE ICCE 2023]

- Accurate expression of theoretical fork rate (a security index) proposed
  - Considering **hash rate**

$$\text{Fork rate } F = \frac{T_w}{T}$$

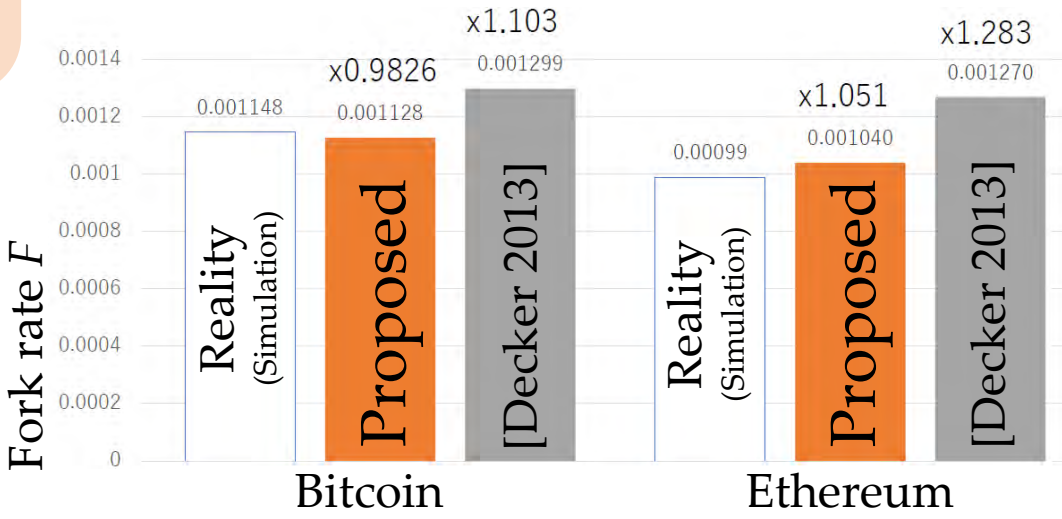
T_w: **Hash rate**-weighted Block propagation time

T: Block generation interval (10 minutes in Bitcoin)



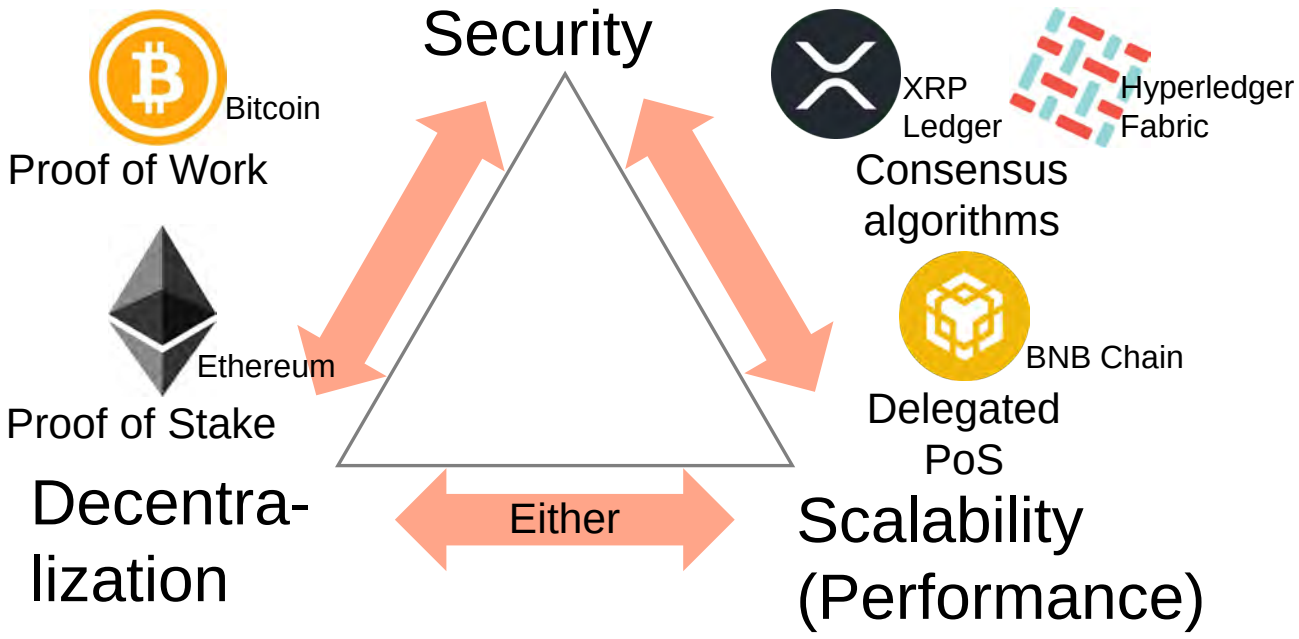
- If by some chance… It expresses the blockchain trilemma?

"Scalability, security and decentralization are not realized simultaneously."



The blockchain trilemma (again)

- Termed by Vitalik Buterin, a founder of Ethereum, in 2017



- We all roughly recognize it.

The blockchain trilemma described in a formula [IEEE Blockchain 2023]

We derived

$$\frac{B_h + B_{tx} \cdot n_{tx}}{T} \cdot \frac{1}{F} \cdot \boldsymbol{H}^\top \boldsymbol{P} \boldsymbol{H} = 1$$

TPS

A term expressing

Scalability (Performance)

Security

Decentralization

Larger variance of H gives smaller value.
Biased H means lower degree of decentralization.

B_h : Size of block header
B_{tx} : Size of a transaction
n_{tx} : Number of transactions in a block

T : Block generation interval
F : Fork rate

$$\boldsymbol{H} = \begin{pmatrix} H_1 \\ H_2 \\ \vdots \\ H_n \end{pmatrix}$$

$$\boldsymbol{P} = \begin{pmatrix} 0 & t_{12} & \cdots & t_{1n} \\ t_{21} & 0 & \cdots & t_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ t_{n1} & t_{n2} & \cdots & 0 \end{pmatrix}$$

H_i : Ratio of hash rate of node i. $\Sigma H_i = 1$

t_{ij} : Propagation time of a block generated by node i to node j / size of a block

- Premise: Proof of Work, fork rate as the security index.
- Future work: Detailed discussion on decentralization, Proof of Stake.

Summary

- Tradeoffs
  - The blockchain **trilemma**
  - **Tradeoff** between performance and security

Hypothetical
[Buterin 2017]

- Research results in our group
  - Tool
  - Scalability (performance)
  - Security

Well-grounded
[Sompolinsky 2015]

- The blockchain **trilemma** described by a formula

Well-grounded
[IEEE Blockchain 2023]