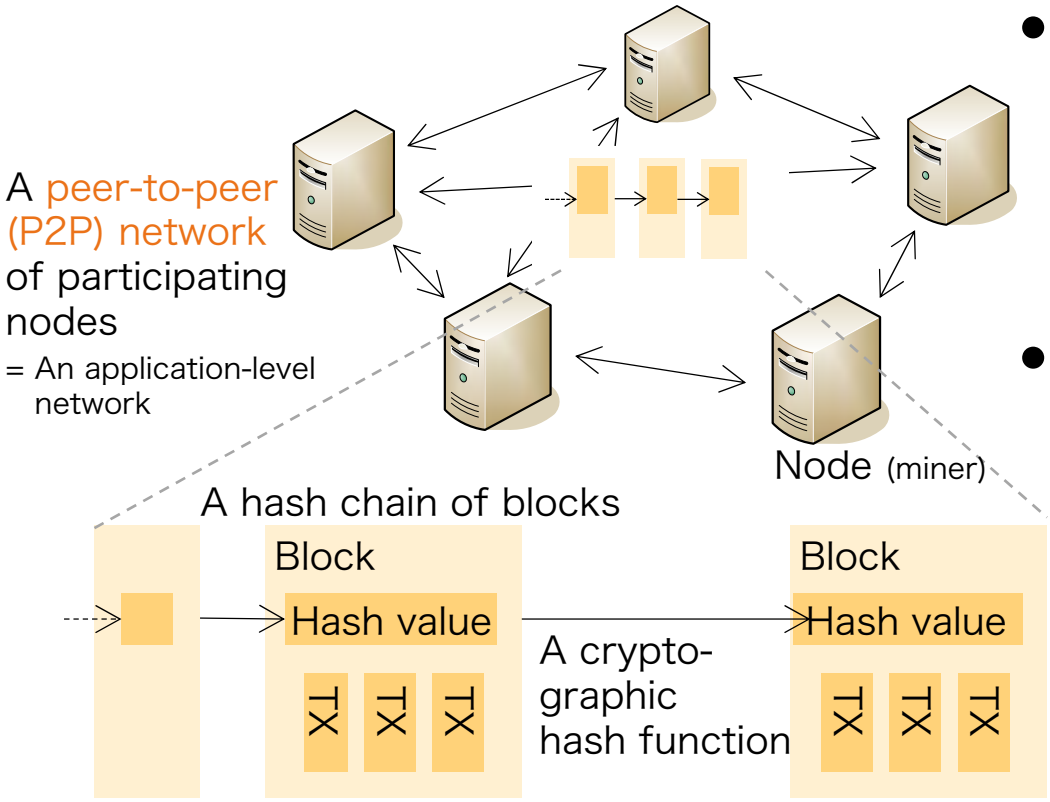
Researches on Blockchain "Networks"

Kazuyuki Shudo
Tokyo Tech
首藤 一幸
東京工業大学

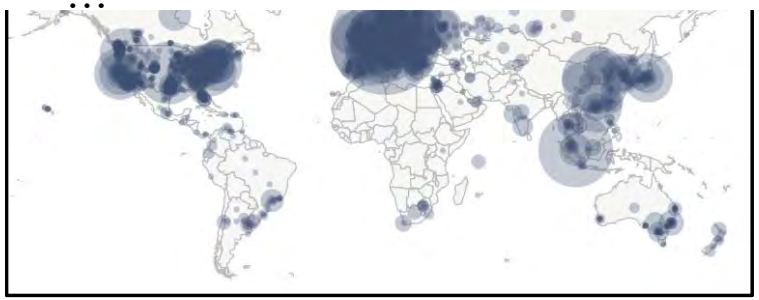
SimBlock

Tokyo Tech

Cryptocurrency and a public blockchain supporting it



- A distributed system supporting cryptocurrencies
  - Bitcoin's market capitalization is US$ 180B.
  - Decentralized
- Expected applications
  - Essentially, time stamp authority or notary office
  - Supply chain mgmt., traceability, governance process such as voting, automatic operation of organizations, …



9,200 nodes on Bitcoin network
https://bitnodes.earn.com/

- Transactions and blocks are broadcasted to all the nodes.
- All the nodes store the identical ledger.
- Nodes race each other for producing a block.
  -> Mining in Proof of Work protocol

Technologies supporting blockchain

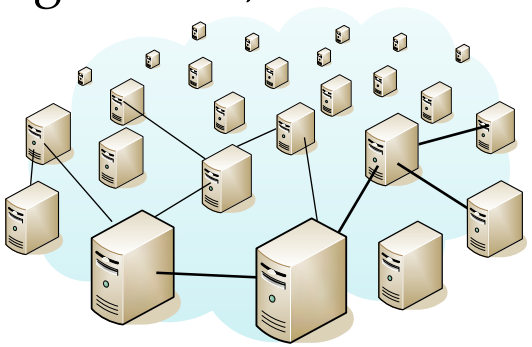
What public (permissionless) blockchains achieved

- Inconsistency (double spending) prevention, and alteration prevention
- Fault tolerance
- Transaction (TX) / data confirmation by a large number of coming and going nodes

Our target

- Cryptography
  - Public-key cryptography, digital signature, cryptographic hash function, random number generation, …

- Distributed systems
  - Peer-to-peer networks, flooding, replication, consistency, consensus algorithms, …



Problems of public blockchains

- Transaction confirmation latency
  - Block generation interval: 10 min in Bitcoin, 15 sec in Ethereum
- Transaction confirmation throughput
  - 7 TX/sec in Bitcoin, -300 TX/sec (est.) in Ethereum
  - 350 TX/sec in PayPal, 1,700 TX/sec in Visa
  - So-called scalability problem ➡ second layer, …

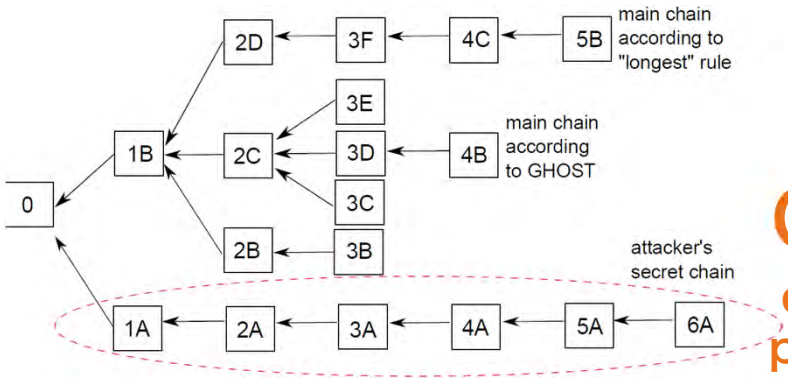
The scope of this talk

- Total amount of data it stores
  - All the nodes store the identical data, > 200 GB
  - Does not scale along # of nodes
    ➡ Downsampling [Li 2019], Distributing with DHT [Abe 2018], …
- Necessity of cryptocurrency operation
  - If the supporting cryptocurrency loses its economic value, nodes run out, the blockchain cannot confirm TXs safely.
    ➡ Portability and migration [Shudo 2018], …

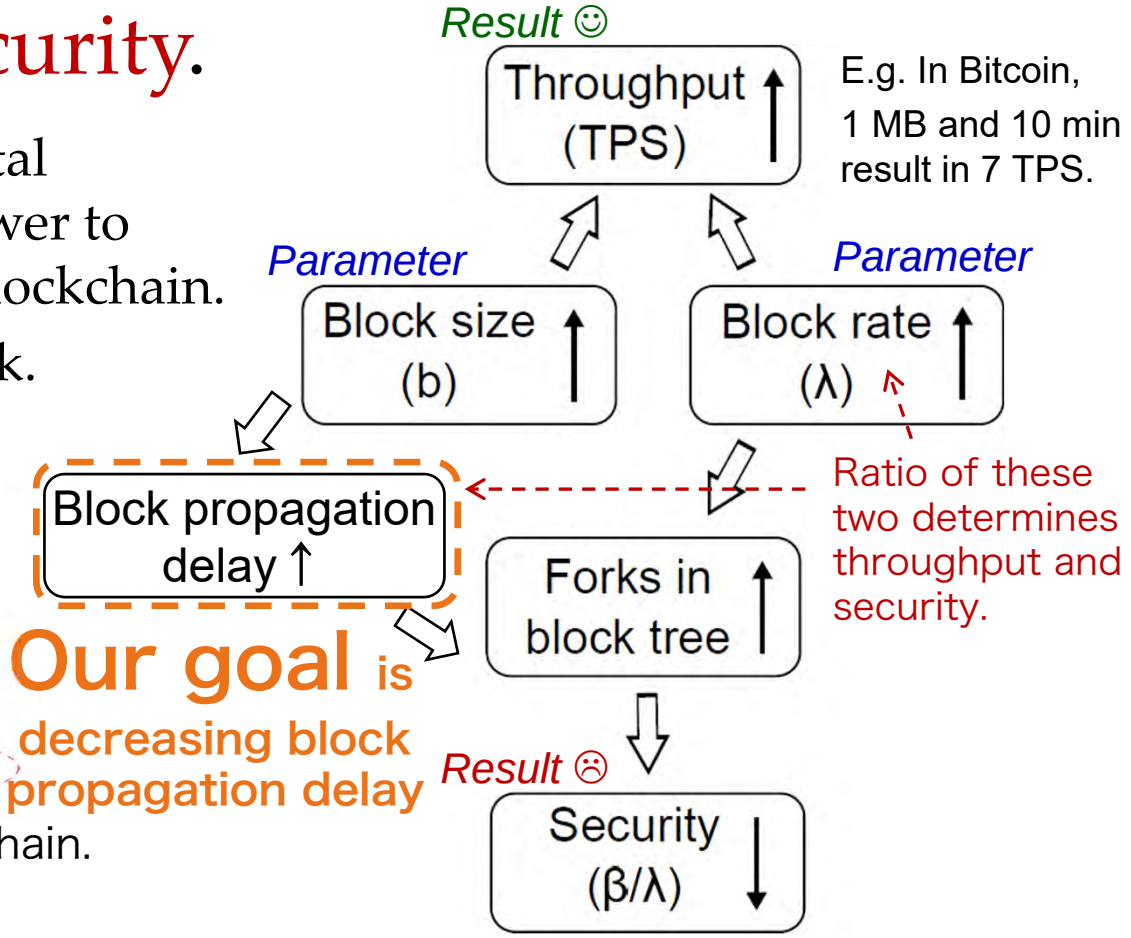
- Number of other interesting problems

Conflict between throughput and security

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



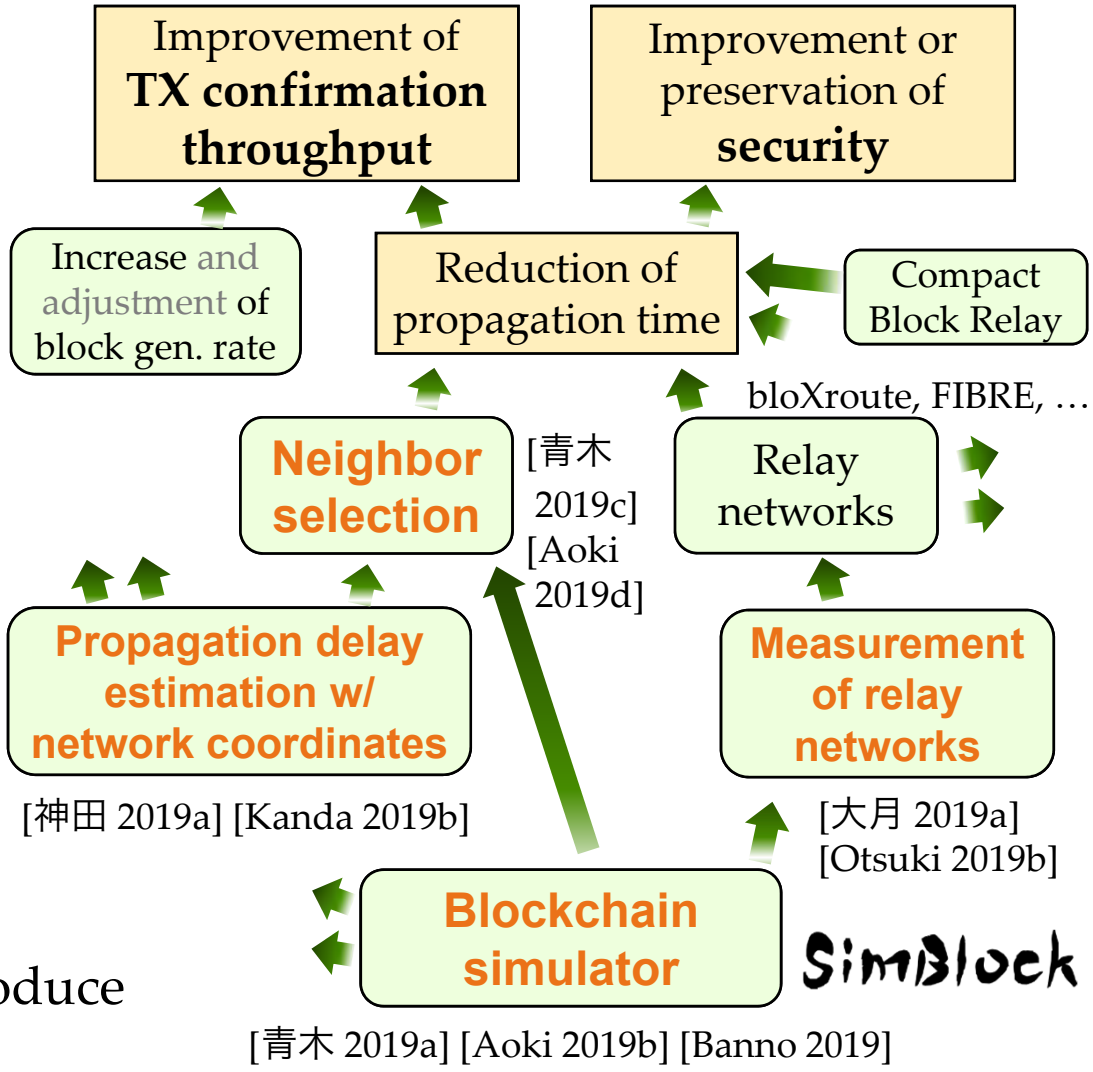
An example of highly forked blockchain.



Figures are from "Secure High-Rate Transaction Processing in Bitcoin", FC'15, 2015

Towards coexistence of performance and security

- Propagation delay estimation with network coordinates
- Blockchain simulator
- Neighbor selection
- Measurement of relay networks

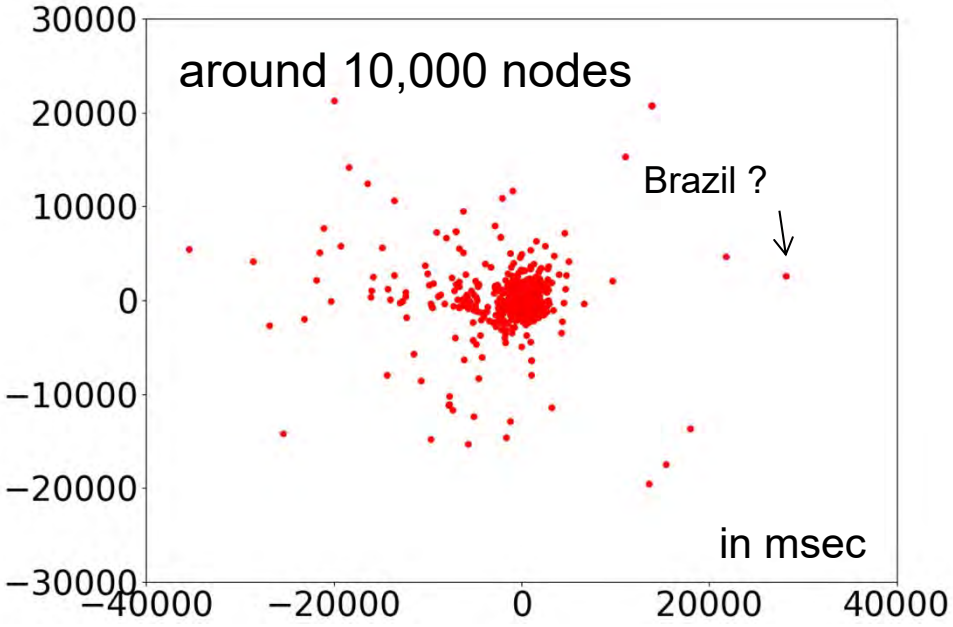


The following slides introduce these activities in order.

Propagation delay estimation with network coordinates

[神田 2019a]
[Kanda 2019b]

- Network coordinates [Dabek 2004] [Chen 2007]
  - is applied to estimated block propagation delay.
  - Determine the coordinates in n-dimensional Euclid space using a physical mass-spring system.



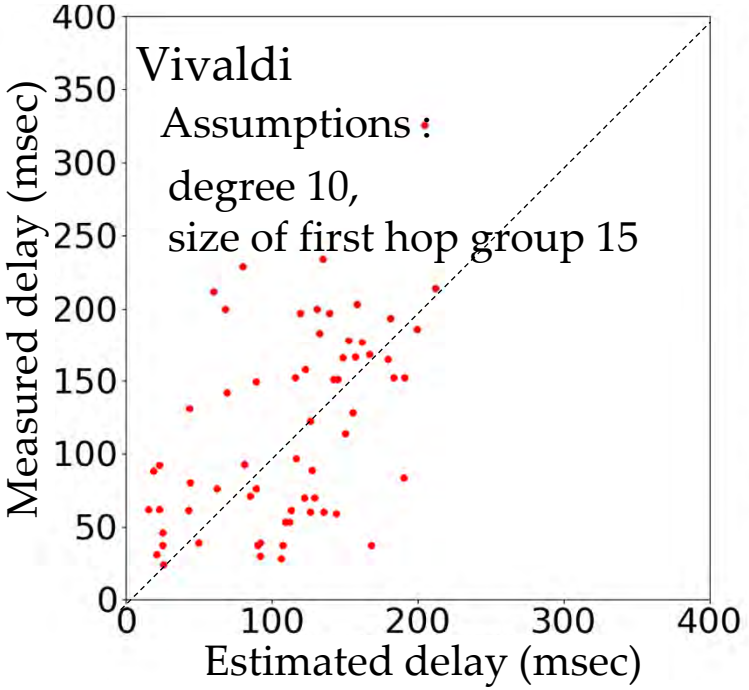
- Purpose: A guide for
  - delay reduction techniques
  - neighbor selection

- But …

Propagation delay estimation with network coordinates

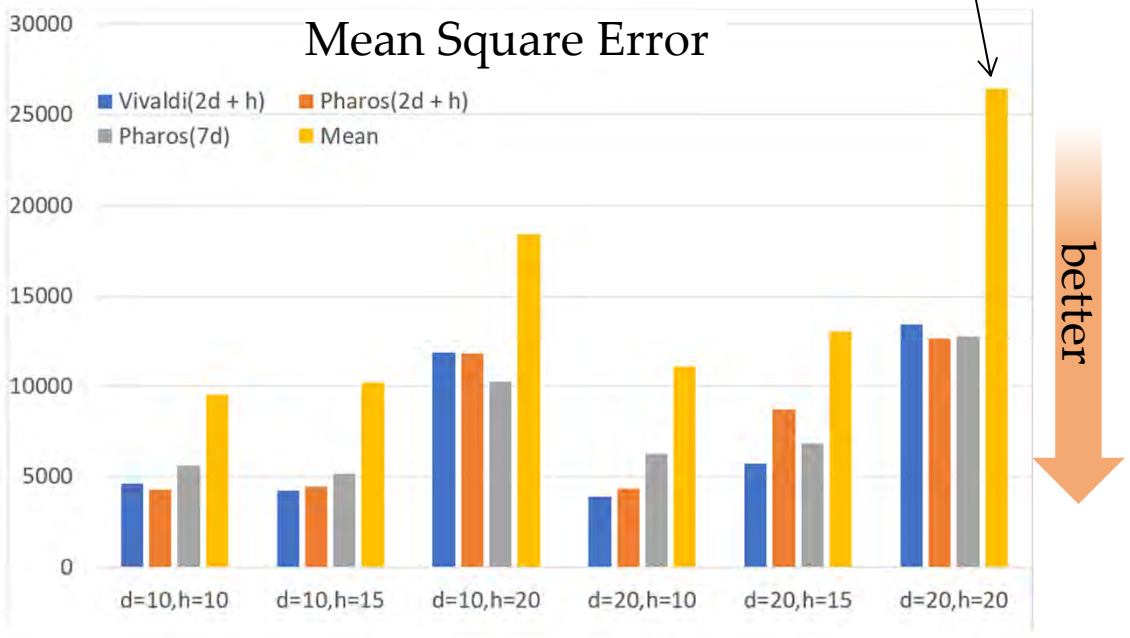
[神田 2019a]
[Kanda 2019b]

- The accuracy is so so.



Measured and estimated delays does not match well ?

In case just using the average



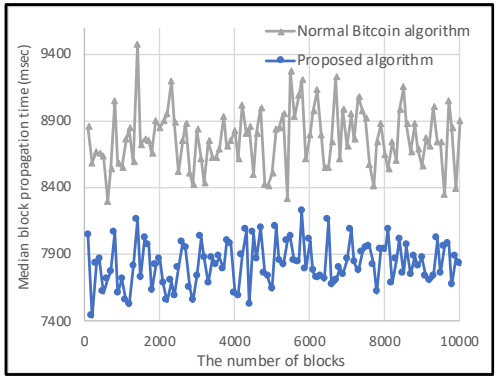
It is not ineffective.

- Lack of topology information is the main obstacle.
  - cf. “TxProbe: Discovering Bitcoin’s Network Topology …”, FC’19, 2019

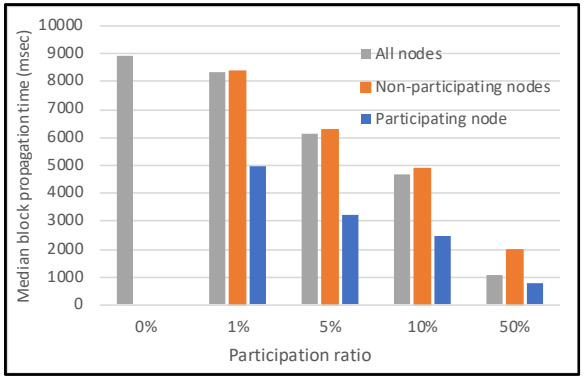
Simulator SimBlock

[青木 2019a] [Aoki 2019b] [Banno 2019]

- A public blockchain "network" simulator
  - developed by Distributed Systems Group, Tokyo Tech, and
  - released in June 2019.
- It simulates transmission of blocks between nodes over Internet, and PoW mining time
  in an event-driven style. It will provides a visualizer.
- It simulates Bitcoin, Litecoin and Dogecoin.
- Researches :



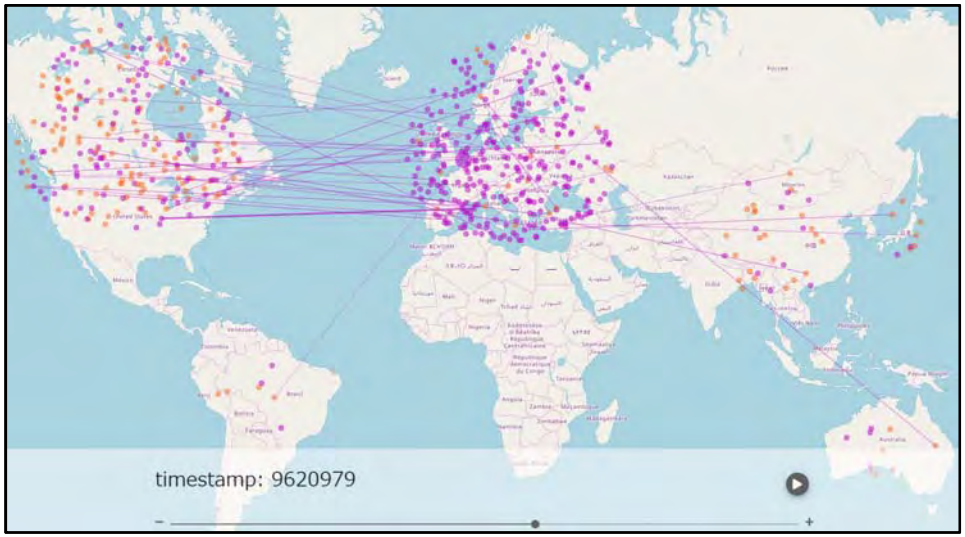
Neighbor selection
[青木 2019c] [Aoki 2019d]



Measurement of relay networks
[大月 2019a] [Otsuki 2019b]

Simulator SimBlock

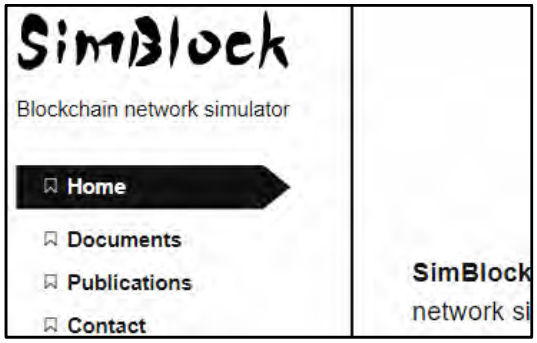
[青木 2019a] [Aoki 2019b] [Banno 2019]

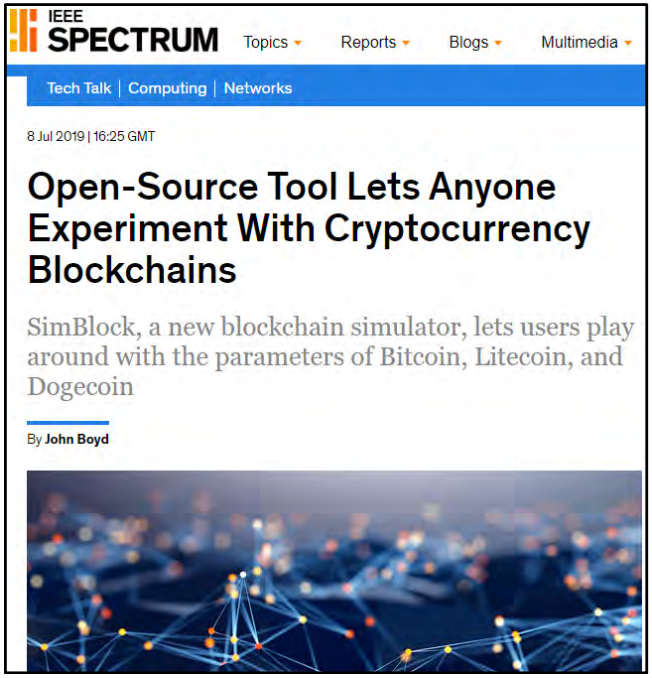


Visualizer

Bitcoin network,
scaled down to 600 nodes for demo

Web site





Article on IEEE Spectrum

Demo
at IEEE ICBC 2019
in Seoul

Proximity Neighbor Selection

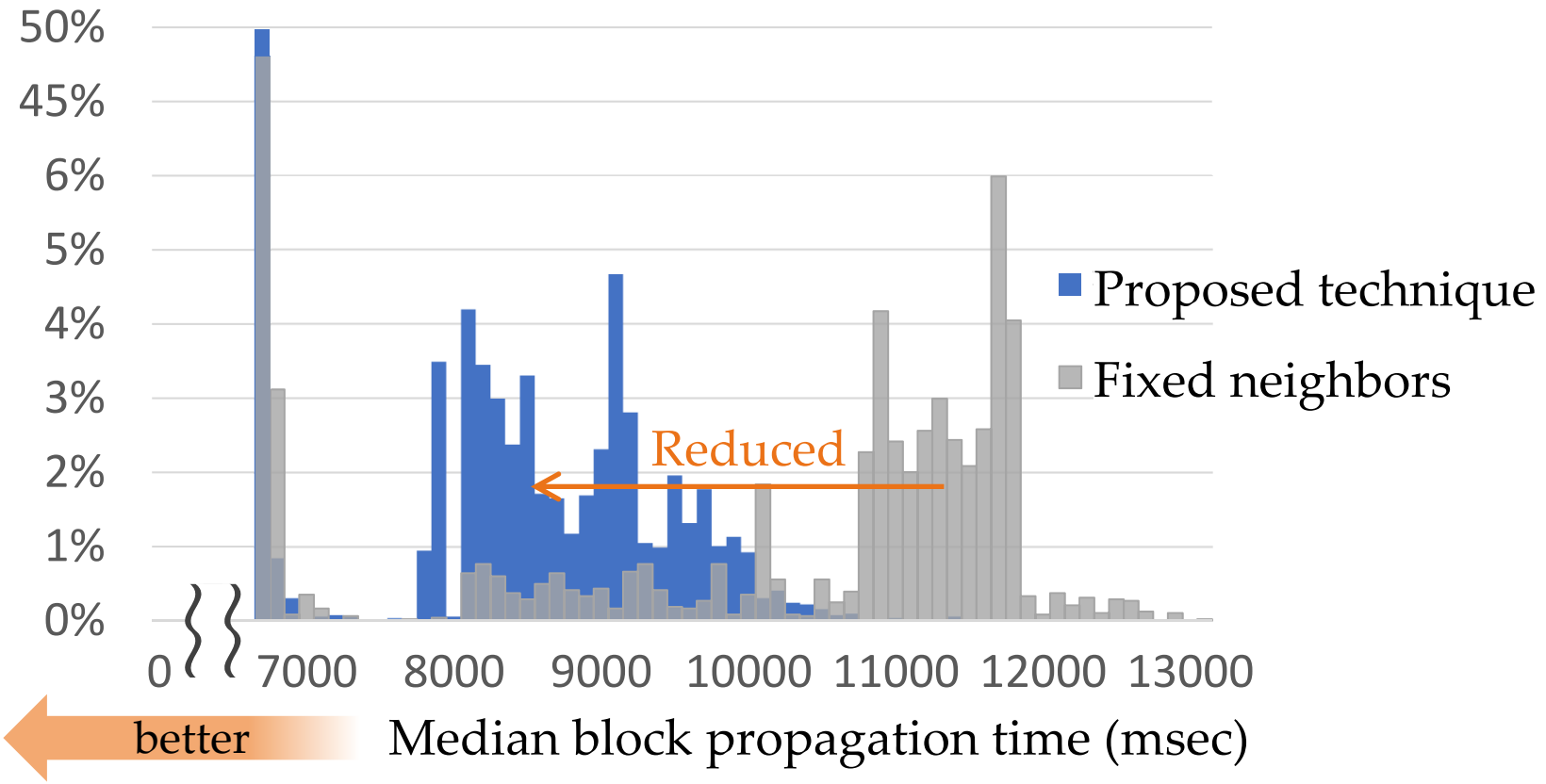
[青木 2019c] [Aoki 2019d]

- Each node selects faster nodes as its neighbors.
  - A major technique in the peer-to-peer field.
    E.g. Our trial for PNS in DHT [ISCC'13].
- Technique
  - Each node scores all the nodes that delivered a block to it.
    - score = time-weighted average of (delivery_time – generation_time) of every blocks
  - A node reselects its neighbors per 10 blocks.
    - But the node selects K nodes randomly from all the nodes it knows.
      Otherwise, a node has no distant neighbors and a block does not go far.
    - K = 1, and P (the weight of the last propagation time) = 0.3
      based on a preliminary experiment

Proximity Neighbor Selection

[青木 2019c] [Aoki 2019d]

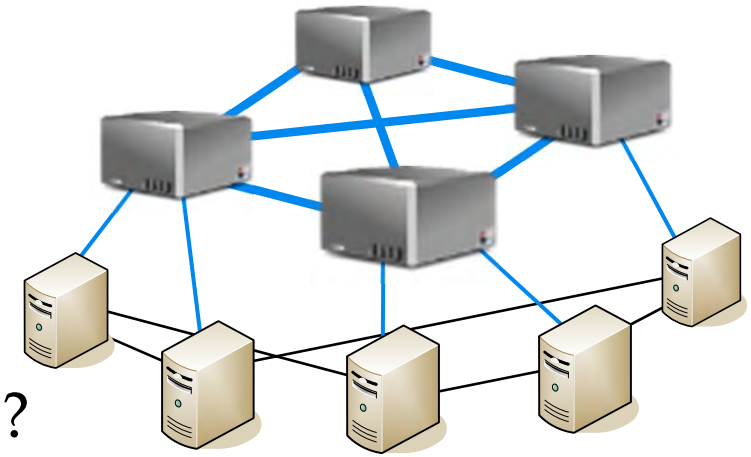
- Reduced from 11.5 sec to 8.5 sec
  for slowly propagated blocks.



Measurement of relay networks

[大月 2019a] [Otsuki 2019b]

- Relay networks
  - Fast block propagation networks
  - bloXroute (2018), FIBRE (2016), Falcon (2016), BFRN (2014), …
  - bloXroute: A business started by Cornell U. guys who have been working on Falcon



A relay network

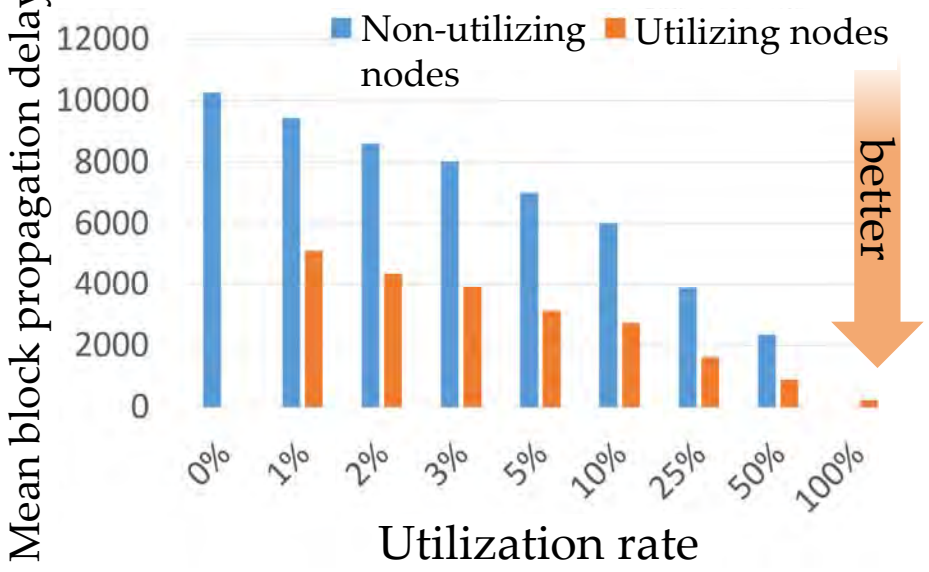
An usual blockchain network

- Effect ?
  - How much does it reduce orphan blocks ?
  - Does it improve mining success rate ?
    (Because a node using a relay network receives blocks earlier.)

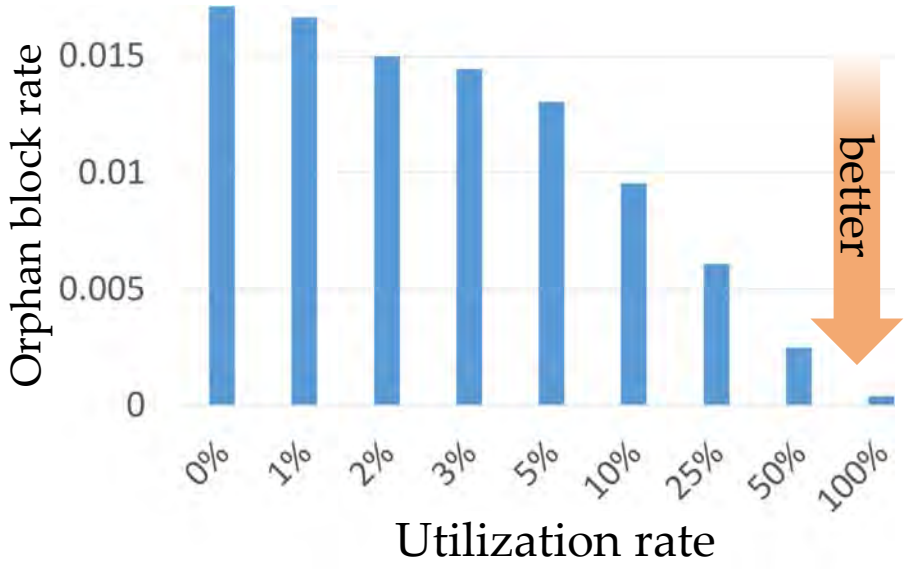
Measurement of relay networks

[大月 2019a] [Otsuki 2019b]

- SimBlock simulates a very fast relay network in addition to a Bitcoin network.
- Network-level :



Faster propagation !



Reduced orphan blocks !

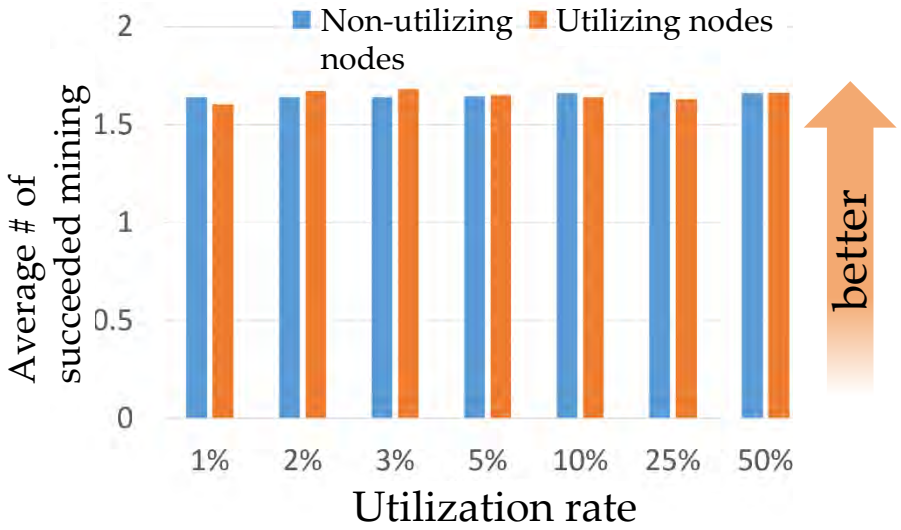
Blocks outside the main chain caused by forks

- So, how about node-level ?

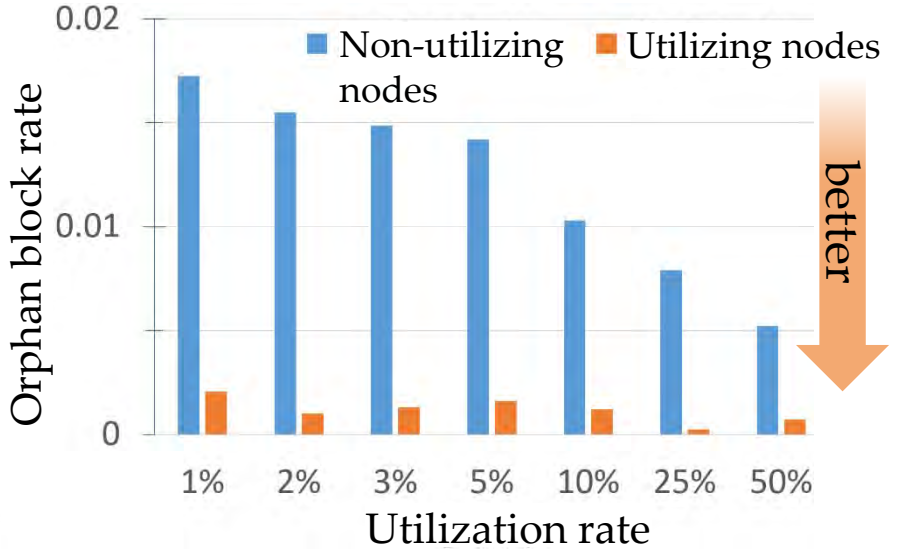
Measurement of relay networks

[大月 2019a] [Otsuki 2019b]

- Node-level :



Mining success rate did not change …



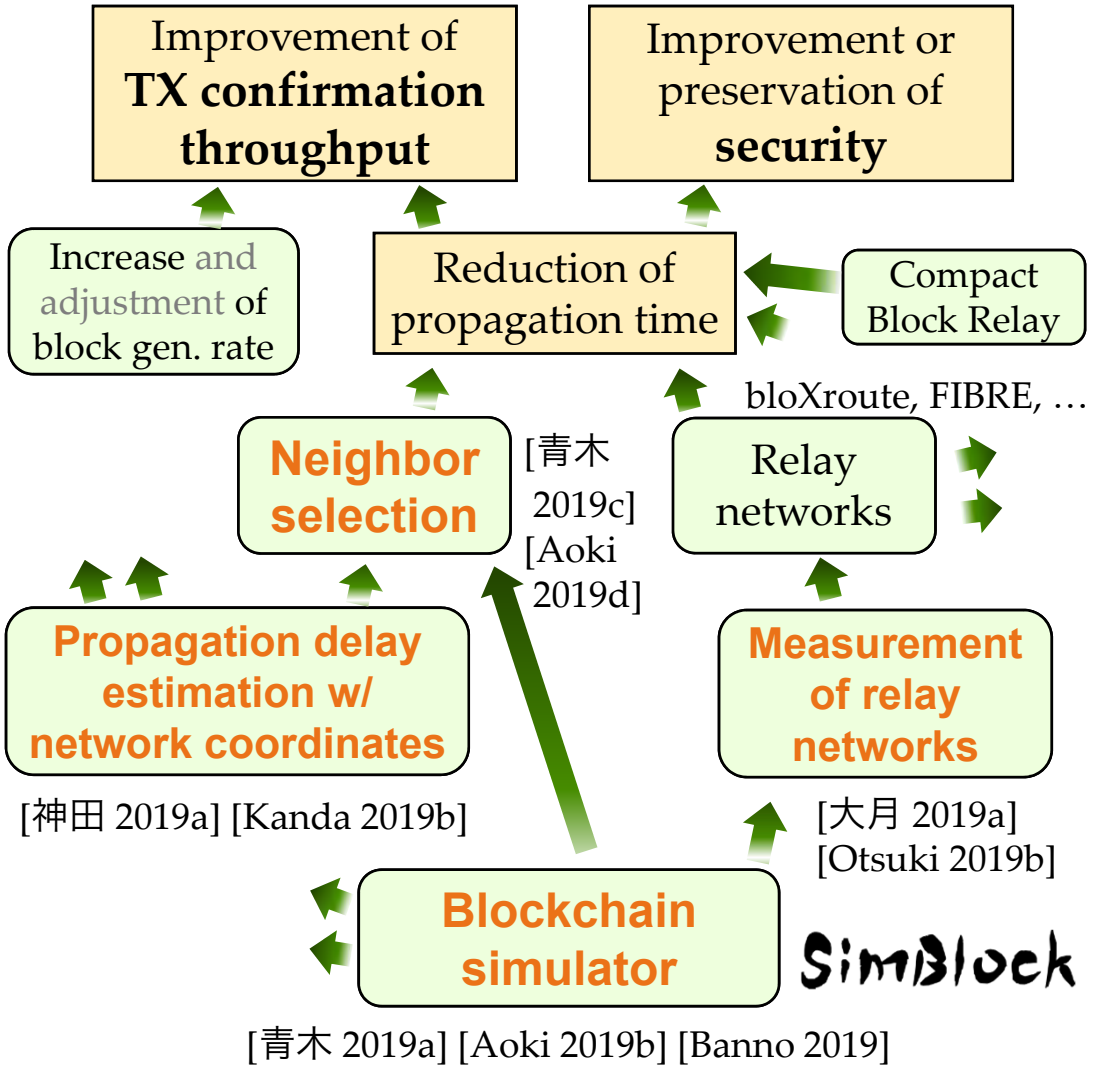
Reduced probability that a block a utilizing node generated becomes an orphan block !

➡ Mining income increased.

A relay network certainly benefits a miner.

Researches on blockchain "network"

- Problems:
  Transaction confirmation
  - delay
  - throughput
- Various trials as the figure on the right
- Acknowledgments
  - This work was supported by SECOM Science and Technology Foundation.
  - The work on delay estimation was supported by Kaula, Inc.



Papers

- Our papers
  - [Shudo 2018] “Towards Application Portability on Blockchains“, IEEE HotICN 2018, August 2018
  - [神田 2019a] “ビットコインネットワーク上でのデータ伝搬遅延推定”, 信学技報, Vol.118, No.481, IA2018-77, pp.317-322, March 2019
  - [Kanda 2019b] “Estimation of Data Propagation Time on the Bitcoin Network”, AINTEC 2019, August 2019
  - [大月 2019a] “Bitcoinネットワークに対するリレーネットワークの影響”, 信学技報, Vol.118, No.481, IA2018-76, pp.309-316, March 2019
  - [Otsuki 2019b] “Effects of a Simple Relay Network on the Bitcoin Network”, AINTEC 2019, 2019年 8月
  - [青木 2019a] “SimBlock: ブロックチェーンネットワークシミュレータ”, 信学技報, Vol.118, No.481, IA2018-70, pp.219-224, March 2019
  - [Aoki 2019b] “SimBlock: A Blockchain Network Simulator“, CryBlock 2019, April 2019
  - [Banno 2019] “Simulating a Blockchain Network with SimBlock“, IEEE ICBC 2019, pp.3-4, May 2019
  - [青木 2019c] “ブロックチェーンネットワークにおける隣接ノード選択”, 信学技報, Vol.118, No.481, IA2018-71, pp.225-232, March 2019
  - [Aoki 2019d] “Proximity Neighbor Selection in Blockchain Networks“, IEEE Blockchain 2019, July 2019
  - [Miyao 2013] “A Method for Designing Proximity-aware Routing Algorithms for Structured Overlays”, IEEE ISCC’13, July 2013
- Papers by others
  - [Li 2019] “Downsampling Blockchain Algorithm”, CryBlock 2019, April 2019
  - [Abe 2018] “Mitigating Bitcoin Node Storage Size By DHT”, AINTEC 2018, November 2018
  - “Secure High-Rate Transaction Processing in Bitcoin”, FC’15, January 2015
  - [Dabek 2004] “Vivaldi: A Decentralized Network Coordinate System”, ACM SIGCOMM 2004, September 2004
  - [Chen 2007] “Pharos: A Decentralized and Hierarchical Network Coordinate System for Internet Distance Prediction”, IEEE GLOBECOM 2007, December 2007
  - “TxProbe: Discovering Bitcoin’s Network Topology Using Orphan Transactions”, FC’19, February 2019