IEEE Blockchain 2019
July 14th – 17th, 2019

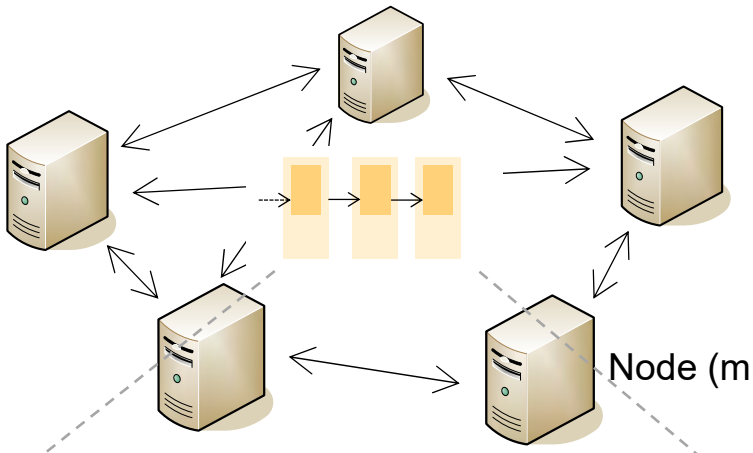
Proximity Neighbor Selection in Blockchain Networks

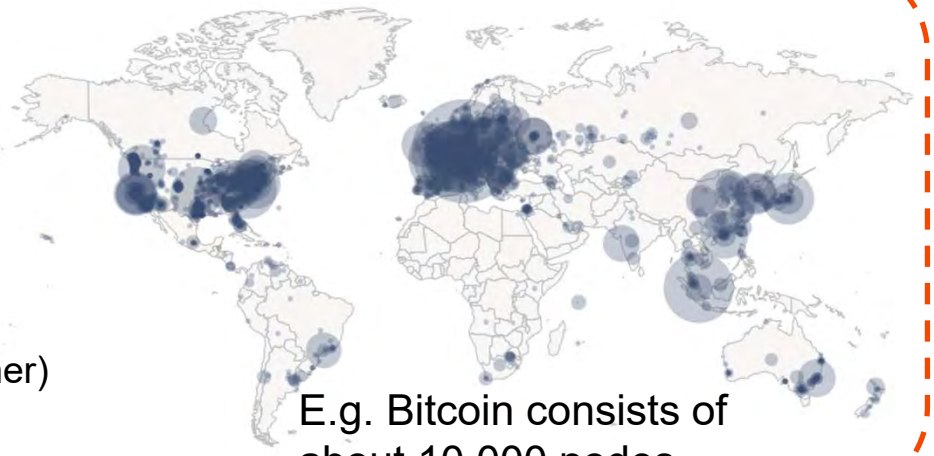
Yusuke Aoki, **Kazuyuki Shudo**
Tokyo Institute of Technology

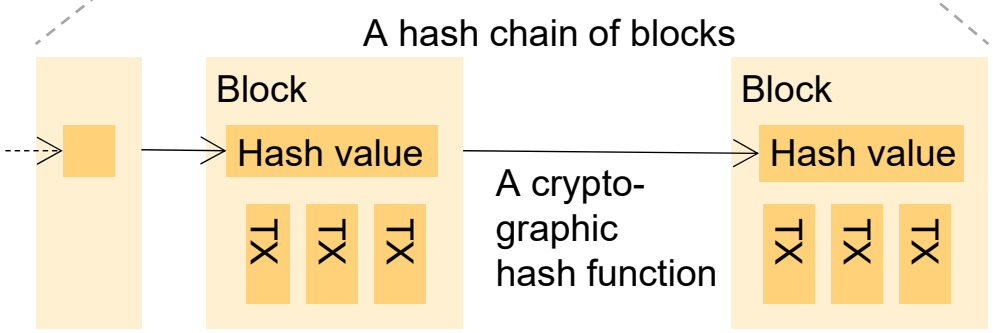
青木 優介, **首藤 一幸**
東京工業大学

Tokyo Tech

A public (permissionless) blockchain is supported by a Peer-to-peer network





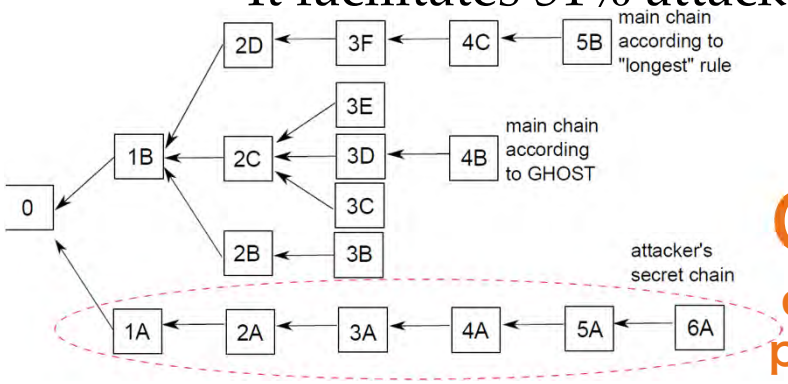


A peer-to-peer (P2P) network of participating nodes

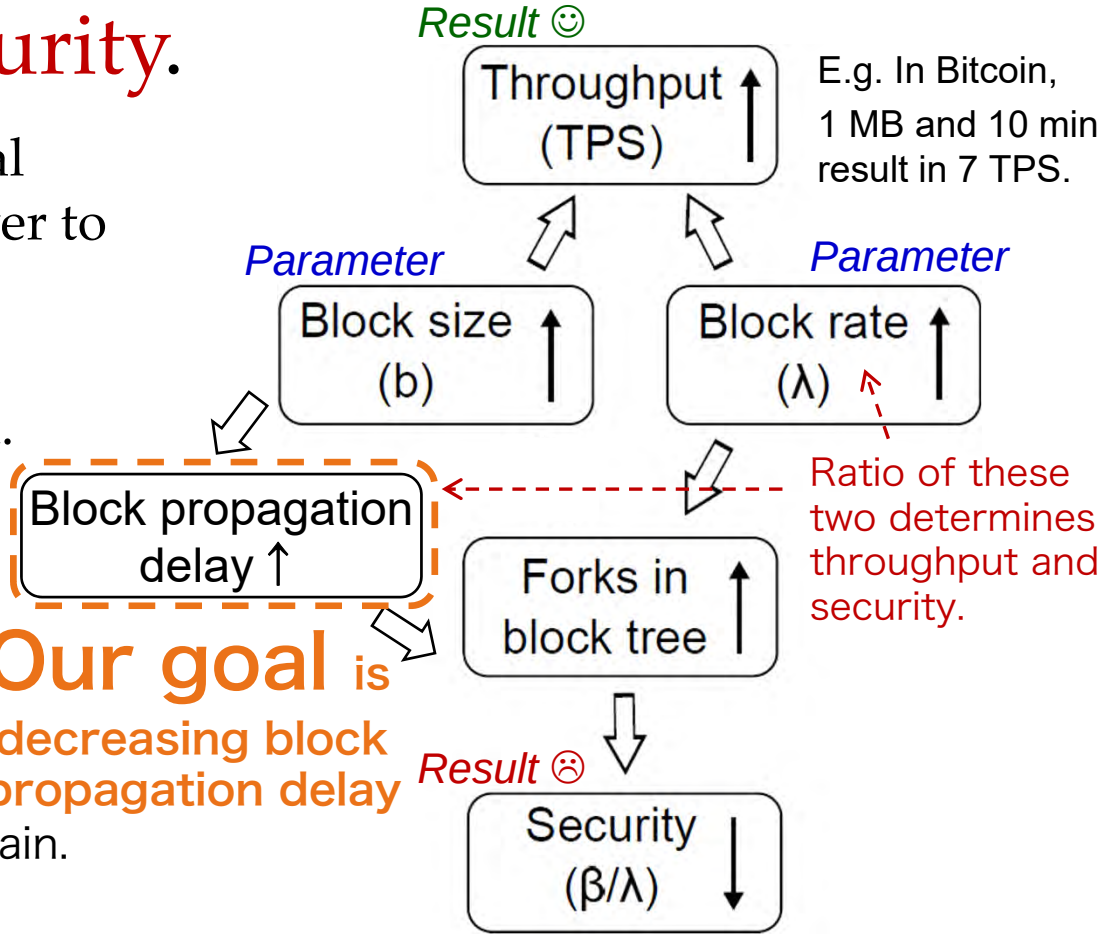
- Transactions (TXs) and blocks are broadcasted to all the nodes.
  - Flooding

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.



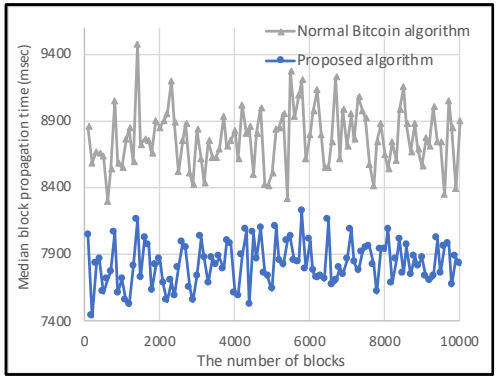
Figures are from “Secure High-Rate Transaction Processing in Bitcoin”, FC’15, 2015

Proposal:
Proximity Neighbor Selection

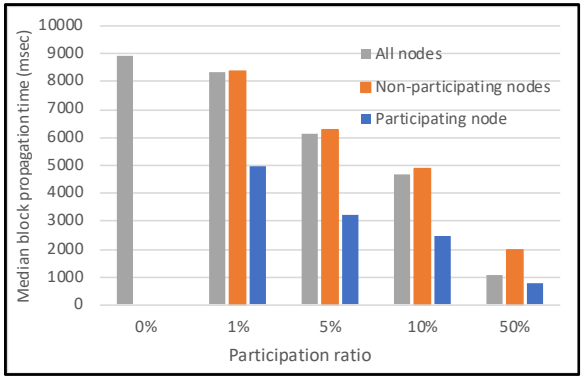
- Each node selects faster nodes as its neighbors.
  - A major technique in the peer-to-peer field.
    E.g. Our trial for PNS in DHT [ISCC'13].
- Technique
  - Each node scores all the nodes that delivered a block to it.
    - score = time-weighted average of (delivery_time – generation_time) of every blocks
  - A node reselects its neighbors every 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

Experimental means:
Simulator SimBlock [CryBlock 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 :



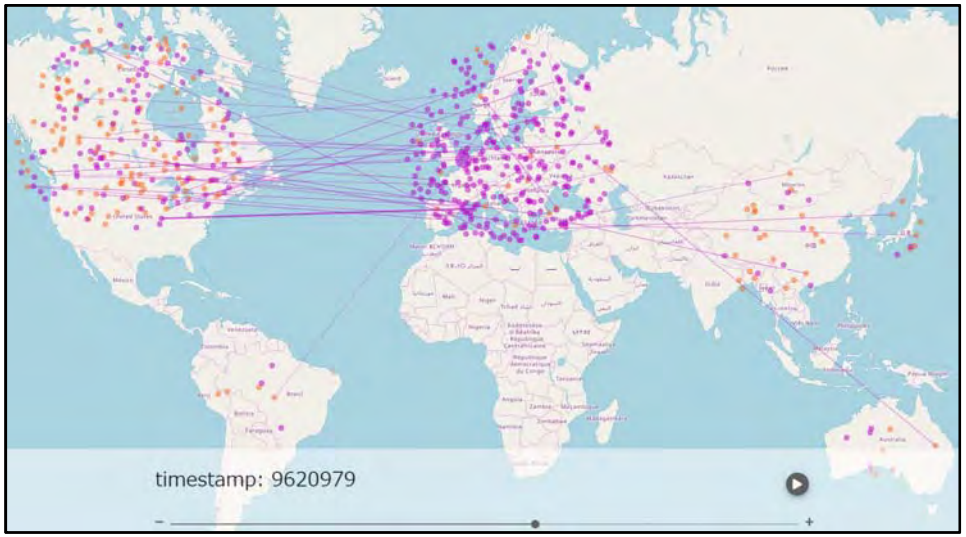
Neighbor selection
[Blockchain 2019]



Measurement of relay networks [AINTEC 2019]

Simulator SimBlock

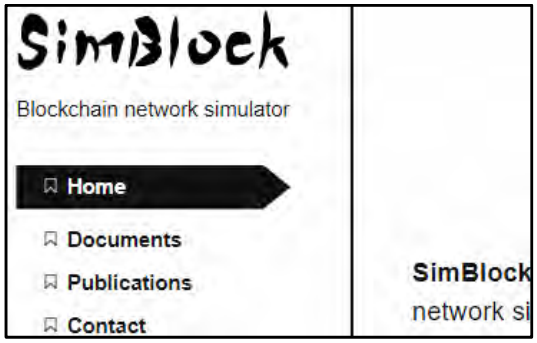
[CryBlock 2019]



Visualizer

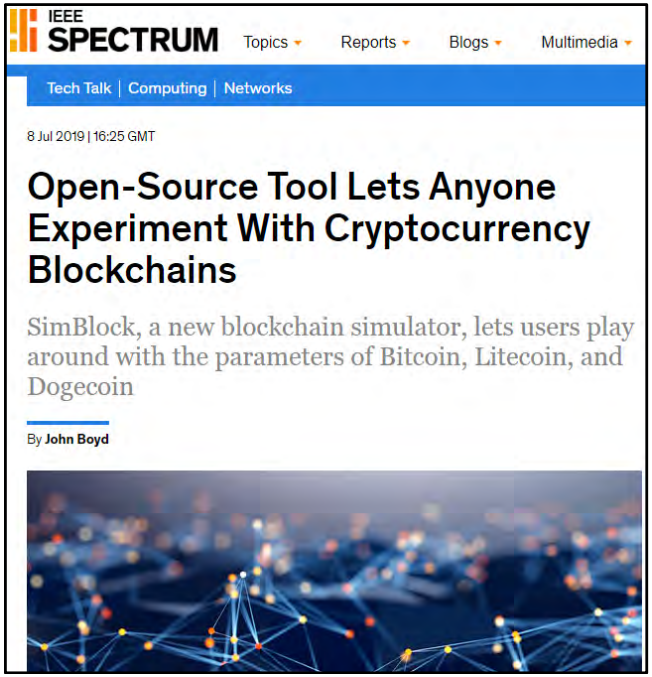
Bitcoin network,
scaled down to 600 nodes for demo

Web site



Demo
at IEEE ICBC 2019
in Seoul

Article on
IEEE
Spectrum



Simulator validation

- SimBlock adopted parameters in [Gervais 2016]
  - "On the Security and Performance of Proof of Work Blockchains", CCS 2016
- Comparison with measured numbers and an existing simulator :

Looks good.

Median block propagation time T_{MBP}

	Bitcoin	Litecoin	Dogecoin
Measured T_{MBP}	8.7 s	1.02 s	0.85 s
[Gervais 2016]	9.42 s	0.86 s	0.83 s
SimBlock	**9.52 s**	**0.78 s**	**0.75 s**

Stale block rate = Orphan (forked) block rate r_f

	Bitcoin	Litecoin	Dogecoin
Measured r_f	0.41%	0.273%	0.619%
[Gervais 2016]	0.14%~ 1.85%	0.24%	0.79%
SimBlock	**1.42%**	**0.25%**	**0.72%**

Experiments

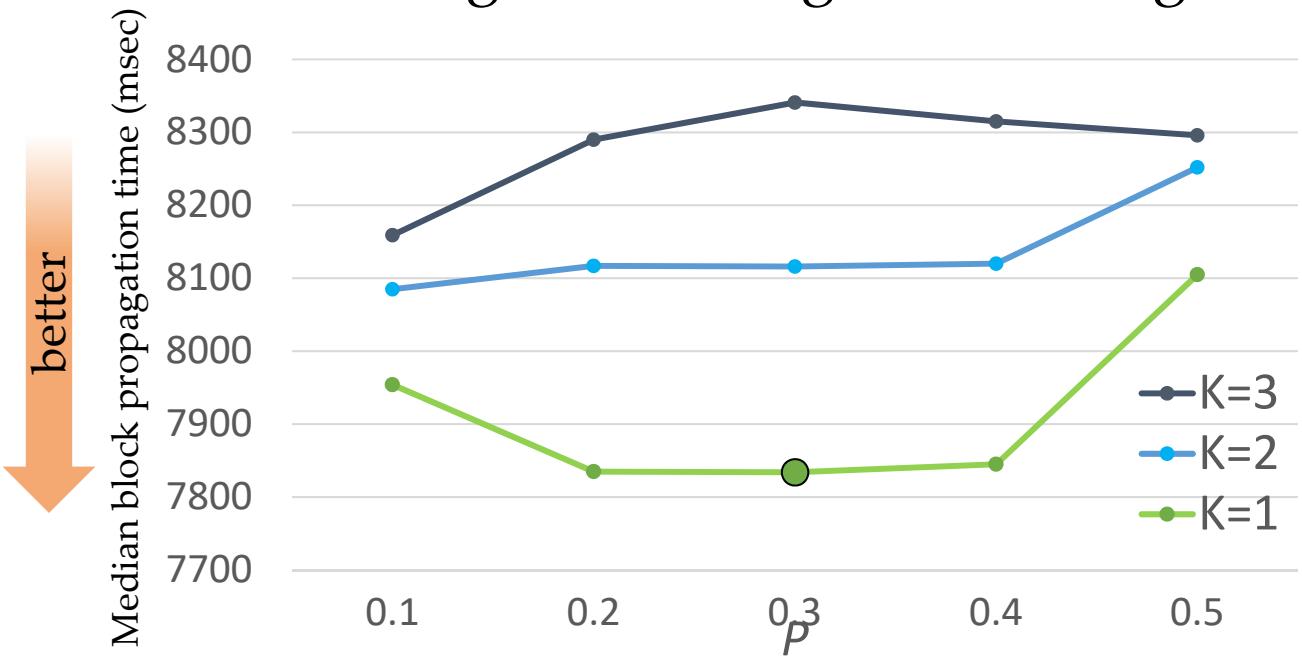
- SimBlock simulates a Bitcoin network with 6,000 nodes.
  - All the nodes run our proposed technique.

Parameter	Bitcoin	Litecoin	Dogecoin
# of nodes	6,000	800	600
Block generation interval	10 min	2 min 30 sec	1 min
Block size	545 KiB	6.11 KiB	8 KiB
# of connections per node	Measured distribution based on [Miller 2015]		
Geographical distribution of nodes	Measured distribution		
Network bandwidth	Measured numbers provided by Verison and testmy.net		
Propagation latency			

[Miller 2015] "Discovering Bitcoin's Public Topology and Influential Nodes", 2015

Preliminary experiment

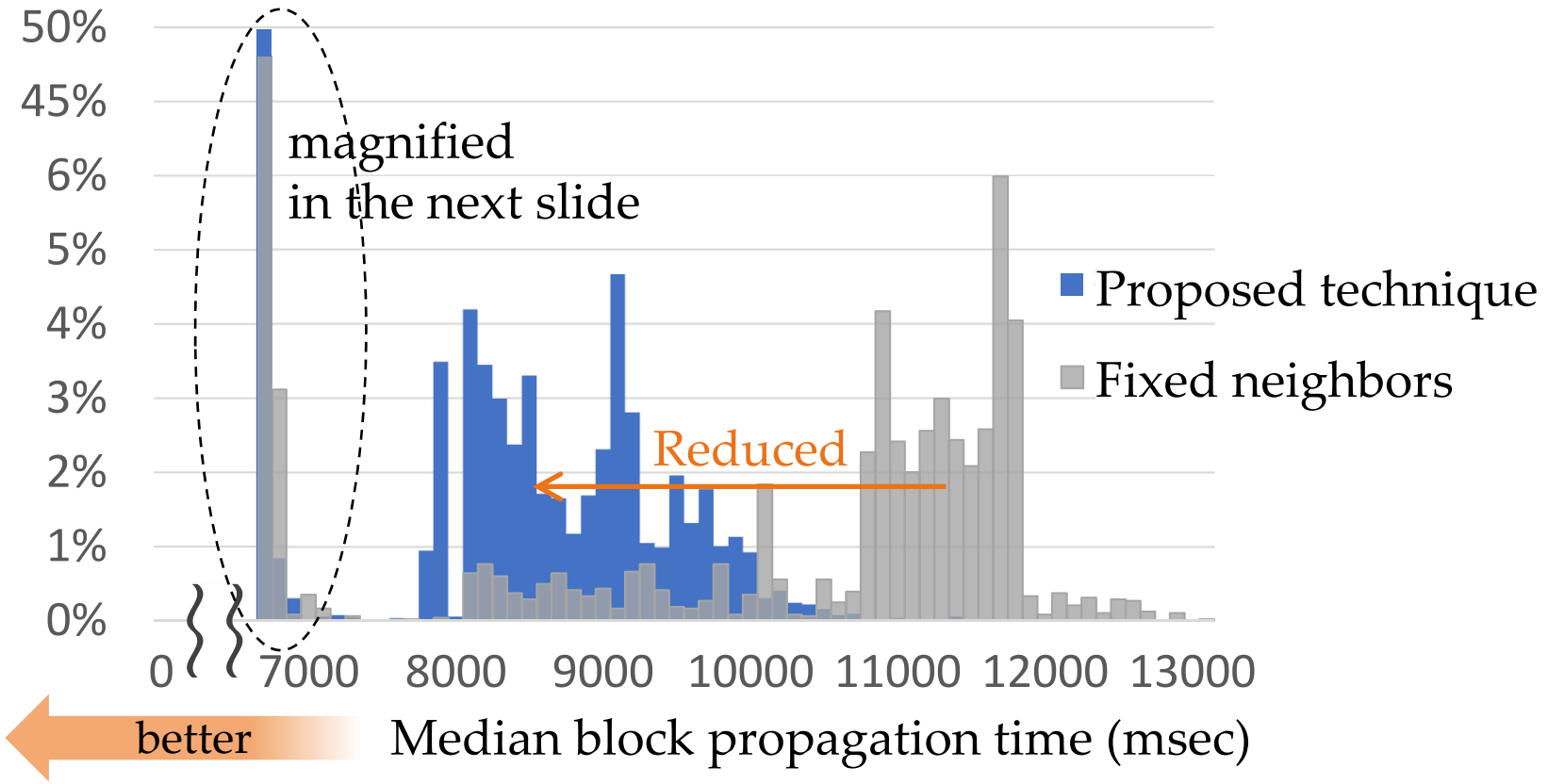
- to determine K and P.
  - K: # of nodes selected as neighbors randomly
  - P: weight of the last propagation time in time-weighted average for scoring



- K = 1, P = 0.3 for the following experiments

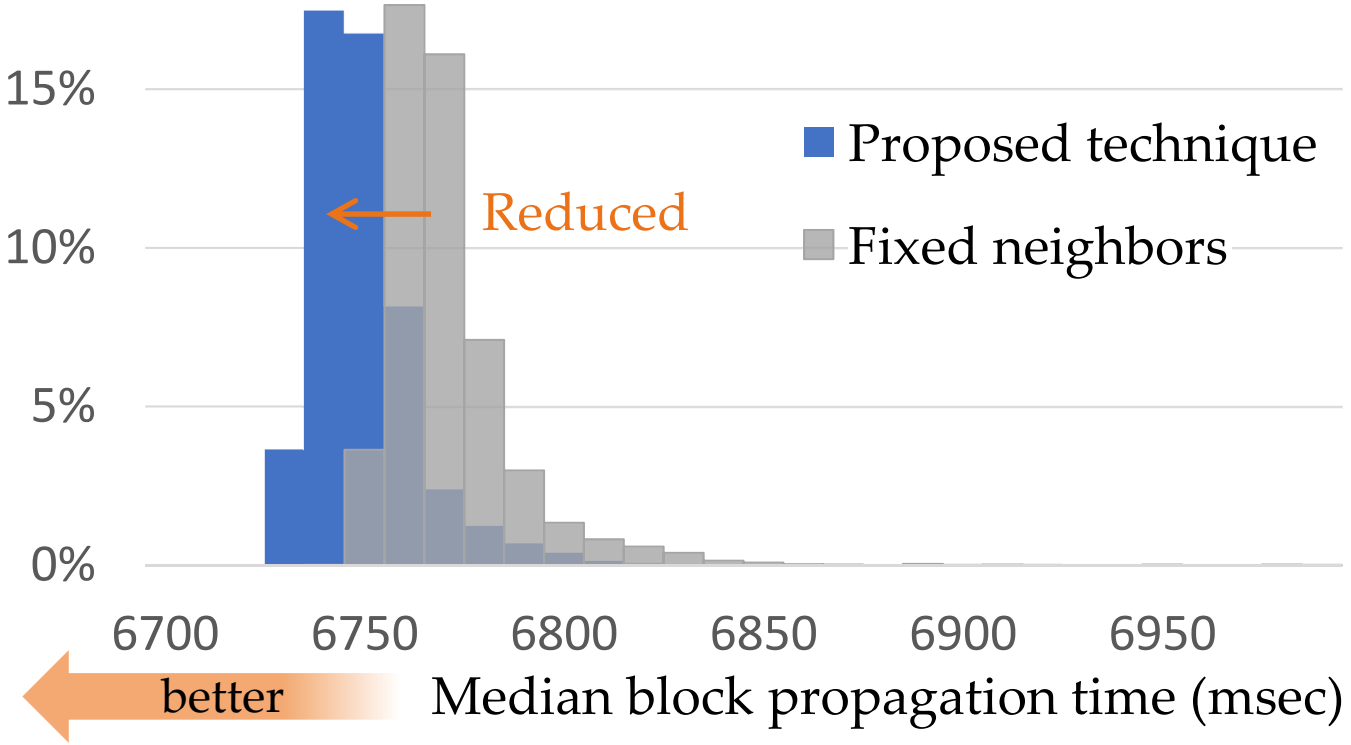
Block propagation time

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



Block propagation time

- Reduced tens of milliseconds
  for fast propagated blocks.



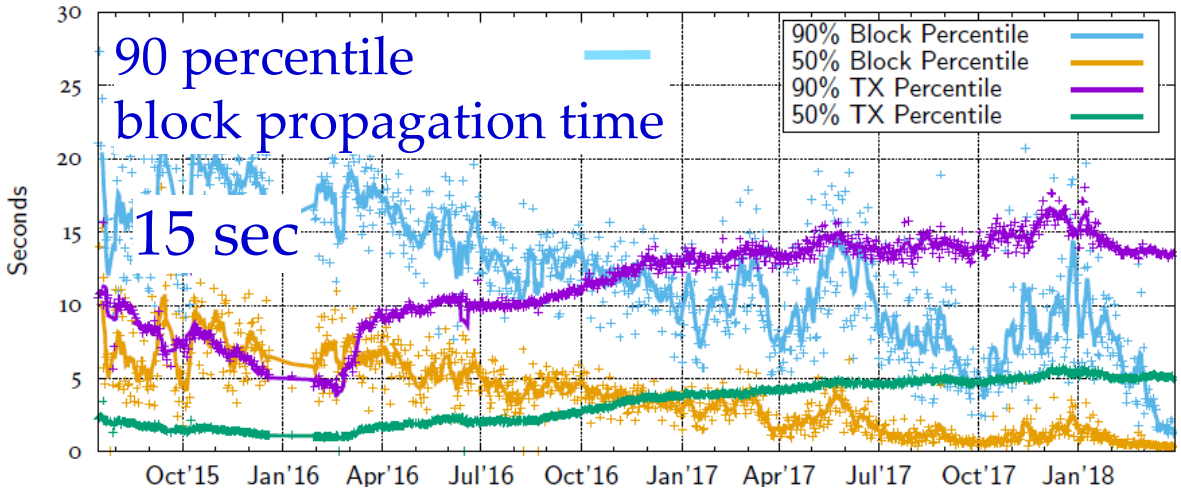
- Similar results shown with uniform block generation performance (uniform hash rate).

Discussion

- Security: Eclipse attack
  - An attacker has to win the block delivery race by delivering blocks fast and fast.
  - It is difficult to fill the K slots, selected randomly.
  - If an attacker starts disturbing delivery, the scores of the attacking nodes decline and they will not be selected as neighbors thereafter.
  - … Further discussion required.

Summary and future work

- Proximity Neighbor Selection works for public blockchain networks.
  - Block propagation time was reduced from 11.5 sec to 8.5 sec.
- Future work
  - Security-conscious / -enhancing neighbor selection
  - Implementing Bitcoin's Compact Block Relay protocol
  - Updating Internet and blockchain parameters



2 sec

Fig. 4.12 in Ph.D. thesis of Till Neudecker

The possible causes of such reduction are **Compact Block Relay** and **relay networks**.