PRESS RELEASE

Source: Tokyo Institute of Technology
For immediate release: June 27, 2019

Subject line: **SimBlock: A simulator for testing improvements to real-world blockchain networks**

Kazuyuki Shudo, his colleagues[a] and the Cybersecurity Research Center at Tokyo Institute of Technology (Tokyo Tech) developed a public blockchain simulator called "SimBlock" for use in testing blockchain performance and security. The software can run on a single PC. It is now publicly available as open source.

SimBlock allows a user to simulate a blockchain network consisting of a large number of nodes (servers), and modify behavior of the nodes to test effects on performance and security. Users can simulate the impact of changes to an existing blockchain, such as Bitcoin, or to a blockchain of their own design.

> SimBlock: A blockchain network simulator
> https://dsg-titech.github.io/simblock/

Background

Blockchain was first implemented for cryptocurrency, serving as the basis of the Bitcoin network, which began operating in 2009. But now other potential applications are being found in areas such as resource and rights management, product (e.g., food) traceability, voting, and business process automation.

These days, a number of conferences on blockchain technology are held, including IEEE ICBC, CryBlock, and IEEE Blockchain. Yet despite the activity in the field, it has been almost impossible to test improvements on a real-world blockchain network. Such an experiment requires updating the software of all nodes, which is not practical for a working network due to the risk of causing disruptions. Even in cases where a blockchain has a problem that needs fixing, testing the fix may be difficult, as it could break something else.

A blockchain simulator called SimBlock

Shudo and colleagues developed SimBlock[1], which can simulate behavior of about 10,000 nodes on the Internet using a single typical PC. The software, which was made open source in July 2019, allows engineers to test improvements on an existing or their original blockchain, or even simulate malicious nodes and measure success rates of attack, then apply countermeasures to test its effects.

SimBlock can currently simulate the parameters of Bitcoin, Litecoin, and Dogecoin, mirroring blockchain network size, block generation interval, and communication speed over the Internet. Users can see what changes to node behavior do to a blockchain network by modifying Java code in SimBlock. It is also possible to modify parameters of the blockchain and communication speed.

SimBlock also has a visualizer that shows communication between nodes and block height[b] animated on a world map. A demonstration of the visualizer is available at the following web page.

Demonstration of visualizer: Bitcoin network (scaled down to 600 nodes)
https://dsg-titech.github.io/simblock-visualizer/
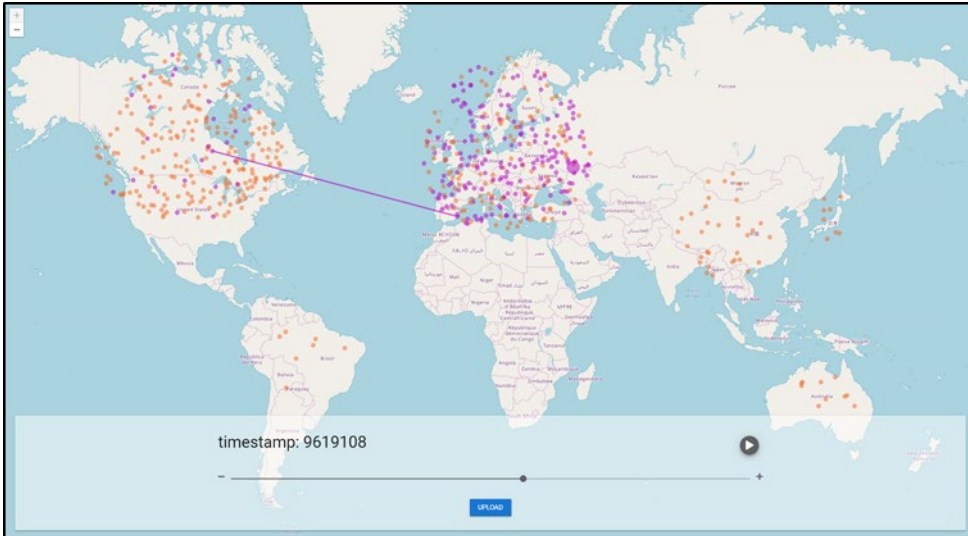
Figure 1. Visualization of a blockchain network, © OpenStreetMap contributors

The research team gave a demonstration of SimBlock[2] at IEEE ICBC 2019 held in Seoul, attracting much attention from the participants (Figure 2).

Figure 2. Demonstrating SimBlock at IEEE ICBC 2019

Application examples

The team members also used SimBlock in their other studies.   The following are such research topics to improve performance of blockchains.

- Neighbor selection [3] (Figure 3)
- Effect measurement of a relay network [4] (Figure 4)

Figure 3 shows the effect of applying a technique called proximity neighbor selection[3], where each node connects with its near nodes on the network. This results in reduced time for blocks to propagate over the network. The reduction of propagation time leads to improvement of security.

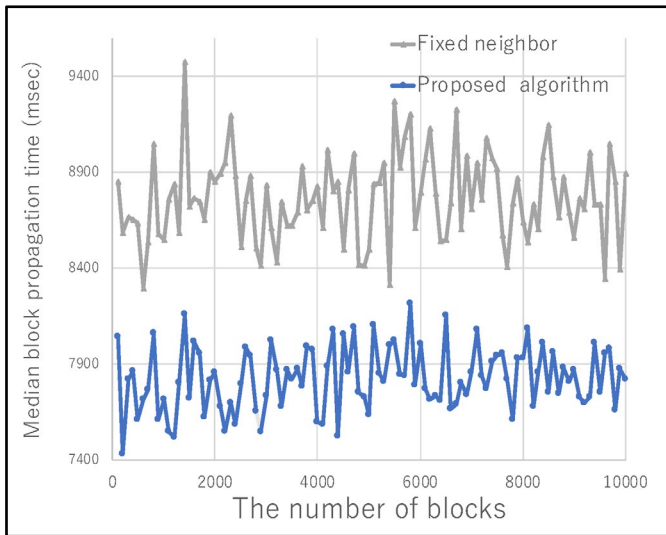It also leads to improvement of transaction process performance without sacrificing security.

Figure 3. Proximity Neighbor selection

Figure 4 illustrates the benefit of nodes utilizing a relay network[c, 4]. By using a relay network, a node can dramatically lower the probability that a block it generated becomes an orphan block[d]. It means that a node can increase its revenue by utilizing the relay network because such an orphan block does not give mining reward to the node that generated the orphan block.

A node utilizing a relay network can receive a newly generated block quickly. It seems that mining[e] success rate of the node increases because of the quick receipt. However, using SimBlock, the research team did not observe any obvious increase. On the other hand, the research team found another benefit of relay networks. A node could lower the probability that a block it generated becomes an orphan block. A relay network naturally lowers the orphan block rate of the entire blockchain network and it has previously been pointed out. The research team found that nodes benefit much from a relay network even if the ratio of nodes utilizing the relay network is very low (e.g., 1%).
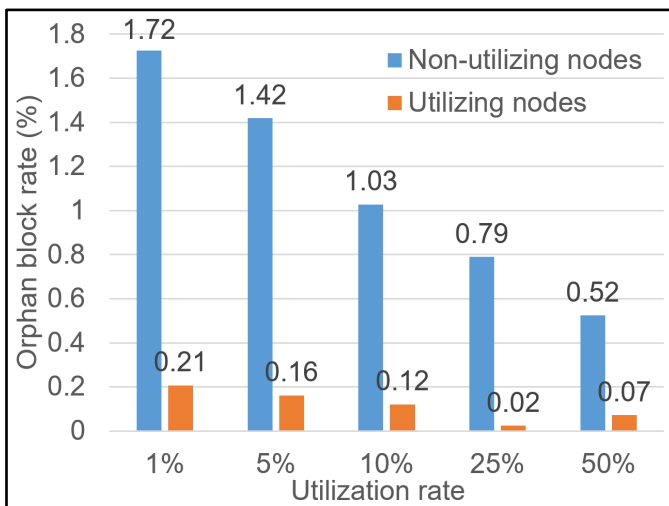

Figure 4. Effect measurement of a relay network

Future plans

The research team will continue working on performance improvement of blockchains utilizing SimBlock. They also started working on security studies by simulating attacks on a blockchain and countermeasures. On-going and planned improvements for SimBlock include support for other blockchains such as Ethereum, further updating of Internet parameters such as communication speed, and support for newer communication protocols such as Compact Block Relay.

The team strongly believes that engineering and research communities can benefit from SimBlock and its contributions to blockchain technology and our society supported by the technology.

Notes

a. Team members: Yusuke Aoki (2nd year master's student in FY 2018), Ryohei Banno (researcher), Takeshi Kaneko (1st year master's student), Ryunosuke Nagayama (1st year master's student), Kai Otsuki (1st year master's student), Kazuyuki Shudo

b. Block height: The length of a blockchain. Here the total number of blocks a node has received.

c. Relay network: A network different from a blockchain network. It distributes blocks and transactions to nodes that connect to it.

d. Orphan block: A block that has been generated once but invalidated due to a fork of the blockchain.

e. Mining: A calculation race between nodes to gain block generation reward.

References

1. Yusuke Aoki, Kai Otsuki, Takeshi Kaneko, Ryohei Banno, Kazuyuki Shudo:
"SimBlock: A Blockchain Network Simulator",
Proc. CryBlock 2019, April 2019

2. Ryohei Banno, Kazuyuki Shudo:
"Simulating a Blockchain Network with SimBlock",
Proc. IEEE ICBC 2019, pp.3-4, May 2019

3. Yusuke Aoki, Kazuyuki Shudo:
"Proximity Neighbor Selection in Blockchain Networks",
Proc. IEEE Blockchain 2019, July 2019 (accepted)

4. Kai Otsuki, Yusuke Aoki, Ryohei Banno, Kazuyuki Shudo:
"Effects of a Simple Relay Network on the Bitcoin Network",
Proc. AINTEC 2019, August 2019 (accepted)

Corresponding researcher
Associate Professor Kazuyuki Shudo
School of Computing, Tokyo Institute of Technology
dsg-titech@googlegroups.com

Contact
Emiko Kawaguchi
Public Relations Section,
Tokyo Institute of Technology
media@jim.titech.ac.jp
+81-3-5734-2975

About Tokyo Institute of Technology
Tokyo Tech stands at the forefront of research and higher education as the leading university for science and technology in Japan. Tokyo Tech researchers excel in fields ranging from materials science to biology, computer science, and physics. Founded in 1881, Tokyo Tech hosts over 10,000 undergraduate and graduate students per year, who develop into scientific leaders and some of the most sought-after engineers in industry. Embodying the Japanese philosophy of "monotsukuri," meaning "technical ingenuity and innovation," the Tokyo Tech community strives to contribute to society through high-impact research.
https://www.titech.ac.jp/english/