Researches on Blockchain “Networks”

Kazuyuki Shudo
Tokyo Tech

SimBlock

首藤 一幸
東京工業大学
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, ...

- 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

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

**Cryptography**

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

**Distributed systems**

- Peer-to-peer networks, flooding, replication, consistency, consensus algorithms, ...

Our target
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, …

• 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], …
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

- **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

- The accuracy is so-so.
  
  Mean Square Error

Measured and estimated delays do not match well?

- Lack of topology information is the main obstacle.
  
  It is not ineffective.

- In case just using the average

Vivaldi Assumptions:
  - degree 10, size of first hop group 15

---

\[\text{Accuracy is so-so.}\]

\[\text{In case just using the average}\]

\[\text{It is not ineffective.}\]

\[\text{Lack of topology information is the main obstacle.}\]

\[\text{cf. “TxProbe: Discovering Bitcoin’s Network Topology …”, FC’19, 2019}\]
Simulator SimBlock

• A public blockchain “network” simulator
  - developed by Distributed Systems Group, Tokyo Tech, and

• 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
  Measurement of relay networks

[青木 2019a] [Aoki 2019b] [Banno 2019]

[青木 2019c] [Aoki 2019d]

[大月 2019a] [Otsuki 2019b]
SimBlock

Simulator

Visualizer

Bitcoin network, scaled down to 600 nodes for demo

Web site

Demo at IEEE ICBC 2019 in Seoul

Article on IEEE Spectrum

Open-Source Tool Lets Anyone Experiment With Cryptocurrency Blockchains

SimBlock, a new blockchain simulator, lets users play around with the parameters of Bitcoin, Litecoin, and Dogecoin

By John Boyd
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 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

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

Median block propagation time (msec)

Proposed technique
Fixed neighbors

Reduced

better
Measurement of relay networks

[大月 2019a] [Otsuki 2019b]

• Relay networks
  – Fast block propagation networks
  – bloXroute: A business started by Cornell U. guys who have been working on Falcon

• Effect?
  – How much does it reduce orphan blocks?
  – Does it improve mining success rate?
    (Because a node using a relay network receives blocks earlier.)
• SimBlock simulates a very fast relay network in addition to a Bitcoin network.

• **Network-level**:
  - Faster propagation!
  - Reduced orphan blocks!

• So, how about **node-level**?

[Mean block propagation delay (msec)]

[Utilization rate]

[Orphan block rate]

[Utilizing nodes vs. Non-utilizing nodes]
Measurement of relay networks

[大月 2019a] [Otsuki 2019b]

• **Node-level:**

  Mining success rate did not change …

  ![Graph showing mining success rate](image1)

  ![Graph showing orphan block rate](image2)

  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.

- Increase and adjustment of block gen. rate
- Reduction of propagation time
- Compact Block Relay
- bloXroute, FIBRE, …
- Neighbor selection
  - [神田 2019a] [Kanda 2019b]
- Propagation delay estimation w/ network coordinates
  - [青木 2019c] [Aoki 2019d]
- Measurement of relay networks
  - [大月 2019a] [Otsuki 2019b]
- Improvement of TX confirmation throughput
- Improvement or preservation of security
- SimBlock

[青木 2019a] [Aoki 2019b] [Banno 2019]
Papers

- **Our papers**

- **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
  - “TxProbe: Discovering Bitcoin’s Network Topology Using Orphan Transactions”, FC’19, February 2019