Tokyo Tech

2019年6月27日

報道機関各位

東京工業大学広報・社会連携本部長
佐藤　勲

パブリックブロックチェーンのシミュレータ「SimBlock」を開発・配布開始

－性能や安全性の手元での検証を可能にし、
ブロックチェーン技術の研究・開発を加速－

東京工業大学 情報理工学院 数理・計算科学系の首藤一幸准教授、青木優介大学院生（研究当時）、大月魁大学院生、金子孟司大学院生、永山流之介大学院生、坂野遼平研究員らの研究グループと情報理工学院 サイバーセキュリティ研究センターは、ブロックチェーンネットワークを PC 上で模擬して性能や安全性を検証できるパブリックブロックチェーンのシミュレータ「SimBlock」を開発し、オープンソースソフトウェアとして公開、無償配布を開始しました。

SimBlock は、インターネット上の多数のノード（サーバ）から成るブロックチェーンネットワークを模擬するソフトウェアです。SimBlock では、ブロックチェーンネットワークを構成するノードの挙動を比較的簡単に変えることができ、改良や新手法がブロックチェーンにどのような影響を与えるのかを PC 上で調べることができます。これによって、Bitcoin といった既存ブロックチェーンの改良や、また、独自に考案したブロックチェーンを手元の PC 上で実験し、その性能や安全性を検証できます。

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

●背景

暗号通貨の基礎技術として生まれたブロックチェーンは、決済や送金だけでなく、資産や権利の管理、また、食料などの流通履歴追跡、投票といった政治プロセス、組織の自動運営などさまざまな応用が期待されています。

2009年のBitcoin立ち上げから開発と展開が先行しましたが、最近では研究も盛

んに行われています。ブロックチェーンを主題とする学術国際会議も、IEEE ICBC、CryBlock、IEEE Blockchain等、いくつも立ち上がっています。しかし、動作しているブロックチェーンネットワークの性能や安全性を高める改良や新手法を考案しても、それを実地で試すことはほとんど不可能です。改良や新手法を試すためには全ノードのソフトウェアを更新する必要がありますが、全ノードの管理者を実験に従わせることは現実的ではありません。そもそもブロックチェーンネットワークの動作を壊してしまうかもしれない実験を実地で行うわけにはいきません。改良や新手法を試せないだけならともかく、もし深刻な問題が見つかって修正したい場合に、修正がネットワークを壊してしまうことがないかどうかを事前に実験・検証できないことも大きな課題でした。

●ブロックチェーンシミュレータSimBlock

そこで本研究チームは、ブロックチェーンネットワークのシミュレータ「SimBlock」［論文1］を開発し、2019年6月、オープンソースソフトウェアとして公開、無償配布を開始しました。SimBlockは一般的なPC上で動作し、1万台近くに達するノード群の、インターネット上での振る舞いをシミュレートできます。技術者・研究者はこのSimBlockを用いることで、Bitcoinといった既存ブロックチェーンの改良や、また、自ら考案したブロックチェーンを、手元のPC上で試すことができます。安全性については、例えば、悪意あるノードを模擬して攻撃の成功率を調べたり、攻撃への対策を模擬してその効果を調べることができます。

現在の SimBlock は、Bitcoin、Litecoin、Dogecoin の、規模やブロック生成間隔、また、インターネット越しのノード間通信時間を模擬できます。ノードの振る舞いを変えたい場合、Java 言語で開発されている SimBlock の当該個所に変更を加えることで、ブロックチェーンネットワーク上で何が起こるかを調べることができます。ブロックチェーンのパラメータ、インターネット上での通信の速さをさまざまに変えることもできます。

また、SimBlock は可視化機能を備えており、ノード間通信と**ブロック高［用語1］**を地図上でアニメーション表示できます（図 1）。技術者・研究者はこの表示から、何が起きているかを直観的に確認できます。以下のウェブページに可視化機能のデモがあります。

可視化のデモ：Bitcoin ネットワーク（デモ用にノード 600 台に簡略化）
https://dsg-titech.github.io/simblock-visualizer/

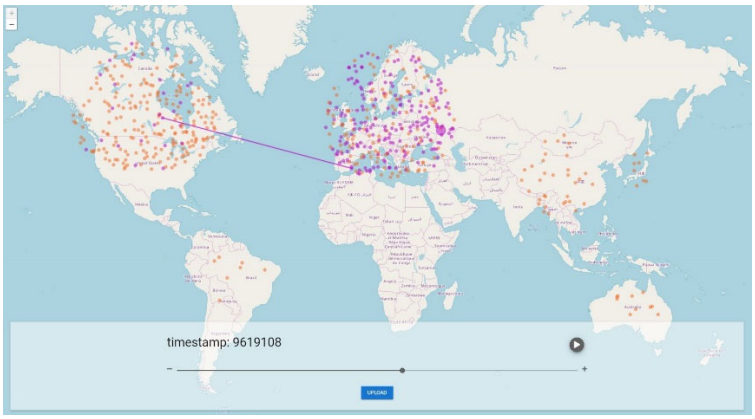

図1　ブロックチェーンネットワークの可視化，© OpenStreetMap contributors

本研究チームは、SimBlockを国際会議IEEE ICBC 2019（2019年5月、韓国 ソウル）にてデモ展示し［論文2］、研究者の関心を集めました（図2）。

図2　国際会議IEEE ICBC 2019でのデモ展示

●応用例

本研究チームは、SimBlockを活用し、ブロックチェーンの性能を向上させる研究を行っています。

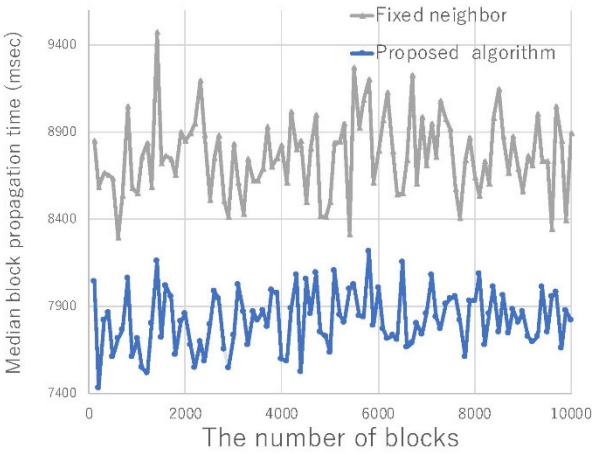

図 3　隣接ノード選択[論文 3，4]

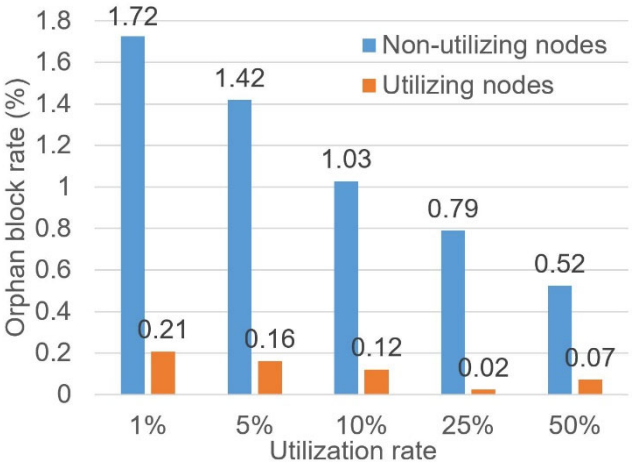

図4　リレーネットワークの影響測定［論文5，6］

図 3 は、隣接ノード選択という技法の効果を示しています。各ノードがネットワーク的に近いノードと優先的に接続を持つように改良することで、ブロックがブロックチェーンネットワーク上を伝搬するのにかかる時間を短縮できました。伝搬時間が短くなると、安全性が向上します。また、安全性を犠牲にせずにトランザクション処理性能を向上させることができます。

図 4 は、**リレーネットワーク［用語 2]**を利用したノードが受ける恩恵を示しています。リレーネットワークを利用することで、**マイニング［用語 3]**によって生成したブロックが**孤立ブロック［用語 4]**になってしまう確率が大幅に下がることがわかりました。これは、リレーネットワークを利用することでノードは収入を増やせることを意味します。なぜなら、ノードは孤立ブロックからはマイニング報酬を得られないからです。

ノードがリレーネットワークを利用すると、生成されたブロックをいち早く受け取れるため、自身がマイニングに成功する確率が上がりそうなものです。しかし、マイニング成功率の明確な向上は確認できませんでした。一方で、本研究チームは、リレーネットワークの利用にはむしろ別のメリットがあることを発見しました。具体的には、マイニングしたブロックが孤立ブロックになって報酬を失う確率を下げることができるという利点です。リレーネットワークによって全体の孤立ブロック発生率が下がることは自然であり、以前より指摘されていました。しかし、リレーネットワークを利用したノードが1%とごくわずかであっても、それら利用したノードは非常に大きな恩恵を受けられるということは本研究チームの発見です。

●今後

本研究グループは、SimBlock を活用してブロックチェーンの性能を向上させる研究を続けていきます。また、ブロックチェーンへの攻撃手法と対策をシミュレートし、安全性を向上させる研究にも取り組んでいきます。SimBlock 自体の改良としては、Ethereum といった他のブロックチェーンへの対応、インターネットの現況への対応、ブロックチェーンの新しい通信方式（例：Compact Block Relay）への対応等を進めています。

SimBlockが、本研究グループの研究だけでなく、多くの技術者・研究者を支え、ブロックチェーン技術の発展とこの技術が支える社会に貢献することを強く信じています。

●謝辞

本研究は公益財団法人セコム科学技術振興財団の研究助成を受けています。

【用語説明】

[用語 1] ブロック高：ブロックチェーンの長さ。ここでは、各ノードがこれまで受け取ったブロックの総数。

[用語 2] リレーネットワーク：ブロックとトランザクションを高速に配布する、ブロックチェーンネットワークとは別のネットワーク。

[用語 3] マイニング：各ノードが、ブロックを生成して報酬を得るために競って行っている計算競争。

[用語4] 孤立ブロック：ブロックチェーンの分岐によって、一度は生成されたものの無効になってしまったブロック。

【論文情報】

[論文 1]
掲載誌：Proc. CryBlock 2019, 2019 年 4 月
論文タイトル："SimBlock: A Blockchain Network Simulator"
著者：Yusuke Aoki, Kai Otsuki, Takeshi Kaneko, Ryohei Banno, Kazuyuki Shudo

[論文 2]
掲載誌：Proc. IEEE ICBC 2019, pp.3-4, 2019 年 5 月
論文タイトル："Simulating a Blockchain Network with SimBlock"
著者：Ryohei Banno, Kazuyuki Shudo

[論文 3]
掲載誌：Proc. IEEE Blockchain 2019, 2019 年 7 月 (採択)
論文タイトル："Proximity Neighbor Selection in Blockchain Networks"
著者：Yusuke Aoki, Kazuyuki Shudo

[論文 4]
掲載誌：電子情報通信学会 技術研究報告, Vol.118, No.481, pp.225-232, 2019 年 3 月
論文タイトル：“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”
著者：青木優介, 首藤一幸

[論文 5]
掲載誌：Proc. AINTEC 2019, 2019 年 8 月 (採択)
論文タイトル："Effects of a Simple Relay Network on the Bitcoin Network"
著者：Kai Otsuki, Yusuke Aoki, Ryohei Banno, Kazuyuki Shudo

[論文 6]
掲載誌：電子情報通信学会 技術研究報告, Vol.118, No.481, pp.309-316, 2019 年 3 月
論文タイトル："Bitcoin ネットワークに対するリレーネットワークの影響"
著者：大月魁, 青木優介, 首藤一幸

【問い合わせ先】

東京工業大学 情報理工学院　数理・計算科学系
准教授 首藤　一幸（分散システム研究グループ）
E-mail: dsg-titech@googlegroups.com

【取材申し込み先】

東京工業大学 広報・社会連携本部 広報・地域連携部門
Email: media@jim.titech.ac.jp
TEL: 03-5734-2975　FAX: 03-5734-3661