一般社団法人　電子情報通信学会
THE INSTITUTE OF ELECTRONICS,
INFORMATION AND COMMUNICATION ENGINEERS

信学技報
IEICE Technical Report
SITE2018-78,IA2018-70 (2019-03)

SimBlock: ブロックチェーンネットワークシミュレータ

青木　優介†　大月　魁†　金子　孟司†　坂野　遼平††　首藤　一幸†††

†, ††, ††† 東京工業大学
〒152-8550 東京都目黒区大岡山 2-12-1
E-mail: †{aoki.y.au,ootuki.k.aa,kaneko.t.ay}@m.titech.ac.jp, ††banno@computer.org, †††shudo@is.titech.ac.jp

あらまし　ブロックチェーンは，中央集権型のシステムを用いずノード群で台帳情報を分散管理する技術として多くの注目を集めている．しかし，実際のブロックチェーンで実験を行うことは，多数のノードを広域に分散して保持する必要があるため困難である．そこで，本研究ではブロックチェーンの研究に用いるシミュレータを開発した．提案シミュレータは既存のシミュレータと異なり，ノードの振る舞いを容易に変更することが可能で，各ノードの動作がブロックチェーンに与える影響を調査することができる．シミュレーション結果と実際のブロックチェーンの測定値を比較し，提案シミュレータの妥当性を示した．また，シミュレータの活用例として，ノードの隣接ノード選択方式を変更した実験及びリレーネットワークへの参加率を変更した実験を行った．シミュレータは数ヶ月後に Web 上で公開する予定である．

キーワード　ブロックチェーンネットワーク，シミュレータ，peer-to-peer

SimBlock: A Blockchain Network Simulator

Yusuke AOKI†, Kai OTSUKI†, Takeshi KANEKO†, Ryohei BANNO††, and Kazuyuki SHUDO†††

†, ††, ††† Tokyo Institute of Technology
Ookayama 2-12-1, Meguro-ku, Tokyo, 152-8552 Japan
E-mail: †{aoki.y.au,ootuki.k.aa,kaneko.t.ay}@m.titech.ac.jp, ††banno@computer.org, †††shudo@is.titech.ac.jp

Abstract　Blockchain, which is a technology for distributedly managing ledger information over multiple nodes without a centralized system, has elicited increasing attention. Performing experiments on actual blockchains are difficult because a large number of nodes in wide areas are necessary. In this study, we developed a blockchain network simulator SimBlock for such experiments. Unlike the existing simulators, SimBlock can easily change behavior of node, so that it enables to investigate the influence of nodes' behavior on blockchains. We compared some simulation results with the measured values in actual blockchains to demonstrate the validity of this simulator. Furthermore, to show practical usage, we conducted two experiments which clarify the influence of neighbor node selection algorithms and relay networks on the block propagation time. The simulator could depict the effects of the two techniques on block propagation time. The simulator will be publicly available in a few months.

Key words　blockchain network, simulator, peer-to-peer

1. はじめに

暗号通貨の基盤技術として登場したブロックチェーンは，暗号通貨以外の分野でも様々な可能性を期待され注目を集めている．ブロックチェーンは，悪意あるノードが複数存在するグループであっても，中央集権のシステム用いずに台帳情報を管理することが可能で，過去のデータの改ざんも困難であるという特徴を持っている．この特徴から多くの暗号通貨で使用され，応用先も広く検討されている．しかし，現状のブロックチェーンは承認時間やスケーラビリティ等の種々の研究課題も存在している．これらの課題について研究する過程で，多くの場合ブロックチェーン上での実験を行う必要がある．しかし，単体のノードで完結するような簡素な実験を除き，ブロックチェーン上で実験を行うことは大きなコストが発生する．ブロックチェーンネットワークは中央的な管理者が存在しない peer-to-peer ネットワークであるため，ネットワーク全体の情

This is an unrefereed paper.

報を取得することはできない．プライベートな実験用のネットワークを構築すれば，ネットワーク全体の情報を取得できるが，多数のノードを用意するコストがかかり，実験の条件やネットワークの構成も容易には変更できないという問題がある．そこで本稿では，ブロックチェーンの研究に用いるシミュレーターを提案する．提案シミュレータはブロックの生成やメッセージの送受信をイベントとするイベント駆動方式のシミュレータである．提案シミュレータは，隣接ノードの選択の仕方を容易に実装できることを目標としている．また，ブロック生成の成功確率からブロック生成時刻を算出しているため，大きな計算能力が必要なマイニングの再現が不要となり，多くのノードが参加するネットワークをシミュレートできる．ブロック生成確率を変更することで様々なマイニングアルゴリズムにも対応できる．2. 章では背景知識としてブロックチェーンの概要を説明する．3. 章では提案シミュレータの説明と評価を行う．4. 章で提案シミュレータの活用例として，隣接ノード選択アルゴリズムを変更した実験及びリレーネットワークへの参加率を変更した実験を行った．5. 章はまとめと今後の課題である．

2. ブロックチェーン

この章では背景知識としてブロックチェーンの概要を説明する．ブロックチェーンは Satoshi Nakamoto 名義で発表された暗号通貨である Bitcoin [1] の台帳部分として考案された分散台帳技術である．ブロックチェーンに参加するノード群が peer-to-peer ネットワークを構築し，台帳情報を共有する．ブロックチェーンには管理者が存在しないため，ノード群で矛盾なく統一した台帳に合意するためのコンセンサスアルゴリズムが考案されている．

2.1 トランザクション伝搬

ブロックチェーンに記録されるデータはトランザクションと呼ばれる．例えば，ブロックチェーンの主な利用先である暗号通貨では，通貨の取引データがトランザクションに当たる．トランザクションの発行者は，ブロックチェーンに参加しているノードを通してネットワークにトランザクションをブロードキャストする．ブロードキャストされたトランザクションは各ノードのトランザクションプールに保存される．このトランザクションはまだ承認前の状態であり，台帳には記録されていない．

2.2 コンセンサス

トランザクションを台帳に保存するために，トランザクションが複数まとめられたブロックと呼ばれるものが生成される．このブロックをブロードキャストすることで，ブロックに含まれたトランザクションは承認され台帳に記録される．各ブロックには直前のブロックのハッシュが含まれており，過去のブロックに含まれているトランザクションの変更するためには，それ以降のブロックを全て書き換える必要がある．このため，新しいブロックを生成するノードを適切に決定する仕組みを採用することで，ブロックチェーンは悪意あるノードが複数存在する可能性のある環境でもトランザクションを改ざんされにくく保存することができる．図 1 のようにブロック同士が直前のハッシュを含むことで，一列につながっていることからブロックチェーンと呼ばれている．

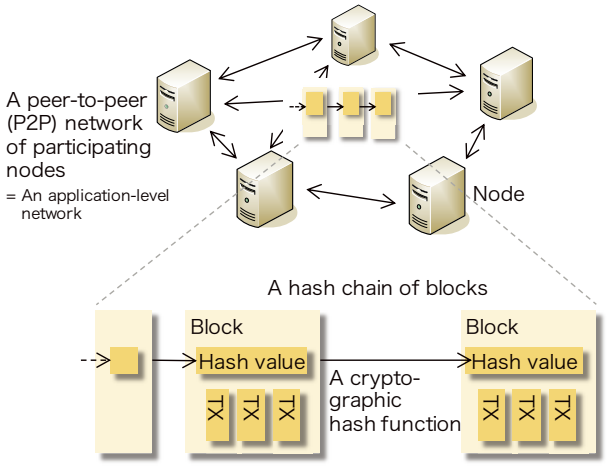

図 1　Blockchain

ブロックを生成するノードの決定するアルゴリズムは数種類提案されている．最も広く知られているアルゴリズムの一つは Bitcoin で提案された Proof of Work (PoW) である．

PoW ではノードの計算パワーに基づいて，新しいブロックを生成するノードを決定する．ブロックにはナンスと呼ばれる各ノードが自由に設定できる値が含まれており，各ノードはこのナンスを変更しながらブロック全体のハッシュ値がある閾値を下回るブロックを探索する．閾値を下回るブロックのみが他のノードに正式なブロックとして受け入れられる．そのため，条件を満たすナンスをより早く発見したノードが，新しいブロックを生成できる．閾値を変更することでブロック生成難易度を調整することができる．ナンスを変更しながらブロック全体のハッシュ値を計算する行為はマイニングと呼ばれている．

PoW ではノードの計算パワーに比例した確率で新しいブロックを生成することができる．ブロックの生成に成功したノードには報酬が支払われるため，ネットワークに参加しているノード間でマイニングの競争が起こり，悪意あるノードが自由に台帳を書き込めないようになっている．

2.3 ネットワーク

ブロックチェーンに参加しているノード同士は peer-to-peer ネットワークを形成している．この peer-to-peer ネットワークでトランザクションやブロックがブロードキャストされる．

ネットワークに参加しているノード同士は定期的に自身の知っているノードの情報を伝達し合う．ノードは新しい隣接ノードが必要な時このノード情報から新しい隣接ノードを選択する．Bitcoin のリファレンス実装である Bitcoin-core [2] では，ノードのネットワークへの参加時や既存の隣接ノードの接続が切れた時などの限られたタイミングでの新規の接続が生成される．そのため，Bitcoin のネットワークのトポロジは短い期間では大きく変化しない [3].

シンプルなプロトコルでは図 2 に示したプロトコルを用いてブロックの送受信が行われている．ブロックを送信するノードは，ブロックを送信する前に INV メッセージを送信し，送信先

のノードがブロックを既に所持していないかを確認する．INV メッセージを受信したノードはブロックを所持していないならば GETDATA メッセージで返答しブロック受信を待つ．このようなプロトコルを用いることで，データ量の大きいブロックの無駄な送信が起きないようになっている．

一つのブロックがネットワーク全体に伝搬し終える前に，異なるブロックが生成されることで，異なる 2 種類のブロックがネットワーク上に伝搬されることをフォークという．フォークが起きると各ノード間で最新のブロックとして異なるブロックを持つことになり，データも整合性がとなくなってしまう．このフォークを防ぐために既存のブロックチェーンでは，ブロックの生成難易度を上げブロックの生成間隔を長くすることで，同時期に複数のブロックが生成されないようにしている．Bitcoin の場合，10 分に一つのブロックが生成される難易度に調整されている．

3. シミュレータ

この章では開発したシミュレータの構成を説明し，既存のシミュレータと比較することで妥当性を評価する．

3.1 構　　成

提案シミュレータは，各参加ノードがメッセージやマイニングをイベントして発生させるイベント駆動シミュレータとした．提案シミュレータでは以下の値をパラメータとしている．

- ブロックパラメータ

  サイズ　ノードによって生成されるブロックのサイズ．

  生成間隔　ブロックチェーンが目標としているブロック生成間隔．
- ノードパラメータ

  ノード数　ブロックチェーンネットワークに参加するノード数．

  次数　各ノードの隣接ノードの個数．

  所在地域　各ノードの所在地域．地域によってネットワークパラメータが決定される．

  ブロック生成能力　各ノードのブロック生成能力．PoW の場合はハッシュレート．全ノードのブロック生成能力の合計とブロック生成間隔の目標からブロック生成難易度が求められる．
- ネットワークパラメータ

  帯域幅　地域ごとの上り帯域幅と下り帯域幅．地域 A から地域 B へメッセージを送信する際の帯域幅は A の上り帯域幅と B の下り帯域幅の最小値とした．

  伝搬遅延　各地域間の電気信号の伝搬遅延の平均値．この値を平均値として分散 20% のパレート分布に従う値を伝搬遅延としている．

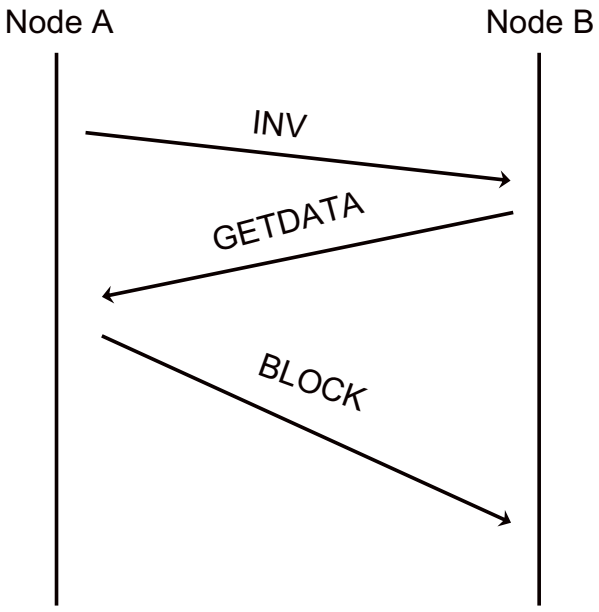

図 2　The protocols when Node A sends block to Node B.

メッセージの到着タイミングを計算するために，地域間の伝搬遅延と帯域幅という二つのパラメータを使用している．メッセージサイズと地域間の帯域幅から転送時間を求め，メッセージの送信イベントから転送時間と伝搬遅延の合計時間後にメッセージ受信イベントを派生させる．今回のシミュレータではブロックのメッセージと比較するとその他のメッセージは十分小さくメッセージサイズは 0 byte としてシミュレートした．

実際のマイニングを再現すると計算量が大きく，シミュレートするノード数を大きくすることができない．そのため，提案シミュレータでは実際のハッシュ計算等のアルゴリズムは行わない．マイニング成功までの時間は全ノードのブロック生成能力の合計とブロック生成難易度から計算する．実際のブロックチェーンでは過去のブロックの生成間隔から各ノードが個々にブロック生成難度を決定しているが，通常の場合，全てのノードで同様の難易度となるため本シミュレータでは全ノードに一意に難易度を与えている．各ノードごとにブロック生成難易度とブロック生成能力からブロック生成成功までの時間の分布を求め，その分布に従う乱数を派生させることで，マイニングイベント終了時刻をシミュレートした．このため，目標ブロック生成間隔と各ノードのブロック生成能力を与えることで，PoW に限らず様々なコンセンサスアルゴリズムに応用することができる．PoW の場合は，ブロック生成の難易度とノードのハッシュレートから幾何分布を求め乱数を発生させている．

本シミュレータは隣接ノードを管理するためのクラスが定義されている．ノードが各メッセージイベントで送受信の対象になった時やブロックの生成に成功した時に隣接ノード管理クラスの対応した関数が呼び出される．この関数を変更することで隣接ノード選択方式を変更することができる．

3.2 評　　価

シミュレータの評価として Grevais ら [4] で紹介されている既存のシミュレータと条件を合わせ比較実験を行った．Grevais らのシミュレータは，ブロックサイズやブロック生成間隔を変更しときに，ダブルスペンディング攻撃等への耐性を調査することを主目的に設計されている．そのため，ブロックサイズ等のパラメータを変更することは容易であるが，ノードのコンセ

ンサスアルゴリズムやネットワークトポロジに関するアルゴリズムを変更することには容易に対応できない．また，実際のブロックチェーンのプロトコルの多くを再現しているため，ノードのアルゴリズムを変更するためには既存のプロトコルに対応するアルゴリズムを全て追加する必要がある．

実験では，Grevais らのシミュレータで用いられているパラメータを再現したとき，シミュレーション結果が同様になることを確かめる．実際の Bitcoin，Litecoin，Dogecoin の環境を再現し，生成されたブロックがネットワークに参加するノードの半数に到達するまでの時間とフォークの発生率を比較する．表 1 のパラメータは Grevais らのシミュレータと同様のものを再現した．

ノード数，ブロックサイズ，ノードの分布地域は Grevais らが 2015 年の実際のブロックチェーンを観測した結果である．ヨーロッパ，北アメリカ，アジア，オーストラリア，日本，南アメリカの 6 地域を設定し，それぞれの地域の帯域幅と伝搬遅延を当時のネットワークを再現して設定している．伝搬時遅延は実地に基づいた平均値をとる分散 20% のパレート分布に従っている．上記の 6 地域に実地データに基づいた分布でノードを配置し，地域間の帯域幅と伝搬遅延をノードに適用している．ノードの次数分布は Miller ら [3] の観測に基づく分布となっている．各ノードは設定された次数個のノードをネットワーク全体からランダムに選び，自身の隣接ノードとする．ノードのブロック生成能力の分布は実際の環境を測定することができない．本実験では，実験では平均の 1/3 の標準偏差をもつ正規分布をブロック生成能力の分布とした．

10000 ブロックが生成されるまでシミュレーションを行った．提案シミュレータと Grevais らのシミュレータの結果，実地データを表 2 に示す．どの値も Grevais らのシミュレータ，実測値に近い値となっており，提案シミュレータは良い精度でブロックチェーンをシミュレートできている．特に同じネットワークパラメータを使用している Grevais らのシミュレータとは非常に近い値をシミュレートできている．パラメータを精査することでより実際の値を正確にシミュレートできる可能性がある．Bitcoin のフォーク率だけは大きな誤差が出たが，これは実験では再現していないリレーネットワークを実際の Bitcoin は用いているためである．

表 1　Grevais らのシミュレータで使用されているパラメータ

パラメータ	Bitcoin	Litecoin	Dogecoin
ノード数	6000	800	600
ブロック生成間隔	10 分	2 分 30 秒	1 分
ブロックサイズ	534 KiB	6.11 KiB	8 KiB
ノード次数分布	Miller ら [3] の観測に従った分布		
ノードの分布地域	実地データを元にした分布		
ネットワーク帯域幅 ネットワーク伝搬遅延	6 地域間の帯域幅，伝搬遅延		

表 2　ブロックの伝搬時間の中央値 (t_{MBP}) とフォーク率 (r_f)

	Bitcoin	Litecoin	Dogecoin
Block interval	10 min	2.5 min	1 min
Measured t_{MBP}	8.7 s	1.02 s	0.98 s
Grevais ら t_{MBP}	9.42 s	0.86 s	0.83 s
提案シミュレータ t_{MBP}	8.94 s	0.85 s	0.82 s
Measured r_f	0.41%	0.27%	0.62%
Grevais ら r_f	1.85 %	0.24%	0.79%
提案シミュレータ r_f	0.78%	0.30%	0.80%

4. シミュレータの活用例

シミュレータの活用の例として，隣接ノード選択アルゴリズを変更した実験とリレーネットワークへの参加率を変更した実験を行った．

4.1 目　　標

既存のブロックチェーンの問題点の一つとして，トランザクションのスループットが低いことがあげられる．ブロックチェーンのスループットは，ブロックに含まれるトランザクション数をブロック生成間隔で割った商となる．ビットコインの場合，一つのブロックに含まれるトランザクション数の上限は約 4000 程度であり，ブロック生成間隔は 10 分であるため，スループットは 7 件/秒程度が上限となっている．このスループットは Visa 平均スループットである約 1700 件/秒 [5] や PayPal 平均スループット約 290 件/秒 [6] と比べると非常に小さなものになっている．

この問題を解決するための方式の一つにブロック伝搬時間を短く改良する方針がある．伝搬時間を短くすることで，ブロック生成間隔を安全に短くしスループットの改善が目指せる [7]．

ブロック伝搬時間を短くするための方法の例を 2 つ示し，その方法を採用したブロックチェーンをシミュレートした．

1 つ目は，ネットワークトポロジの効率化を試みる方法である．2. 章で触れたように，ブロックチェーンのネットワークは中央管理者が存在しない P2P ネットワークである．そのためネットワークのトポロジは個々のノードの隣接ノードの選択の仕方によって変化する．トポロジを効率化する選択アルゴリズムを提案し，その効果をシミュレータ上で測定する．2 つ目は，ブロックチェーンで用意されたネットワークとは別のブロック伝搬専用ネットワークを用意する方法である．既存研究として bloXroute [8] や Falcon [9] がブロック伝搬専用のネットワーを提案し，ブロック伝搬の効率化を図っている．このようなリレーネットワークの効果を測定するため，シミュレータ上でリレーネットワークへのノードの参加率を変化させながら伝搬時間を観察する．

4.2 隣接ノード選択アルゴリズム

提案アルゴリズムでは，ブロックの INV メッセージをより早く送信したノードを優先して接続するように設計した．各ノードは自身に INV メッセージを送信したノードにスコアをつけ，接続する優先順位を決定する．各ノードは INV メッセージを受信するたびに，そのブロック生成時刻からの経過時間を記録する．10 ブロックを受信するたびに，各ノードは上記の記録した経過時間の平均に基づいて隣接ノードの更新を行う．INV メッセージを送信してきたノードごとに，記録していた経過時間の平均をとり，各ノードのスコアとする．スコアの小さいもから

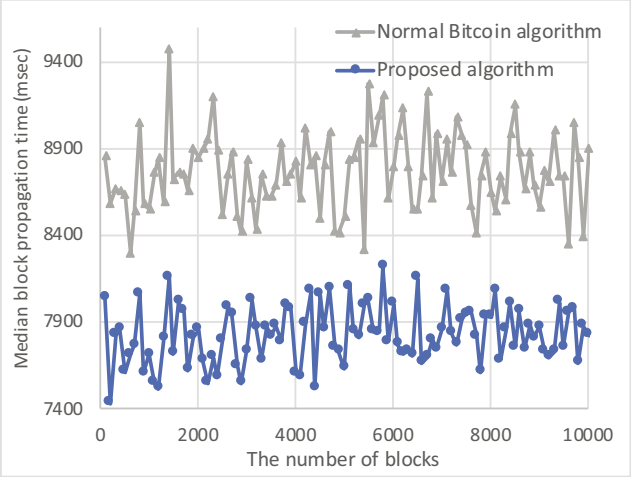

図 3　The median of block propagation time

順に新たな隣接ノードとしてコネクションを張る．ただし，新しいノードの情報を入手するために 1 個の隣接ノードは全ノードから一つをランダムに選択される．

シミュレータのパラメータは 3. 章の Bitcoin と同様の条件で行った．通常の Bitcoin ノードと同様で隣接ノードが固定されているノードのみが参加するネットワークと提案ノード選択アルゴリズムを採用しているノードのみのネットワークのブロック伝搬時間の中央値を比較する．図 3 に生成されたブロック数を横軸にとり，伝搬時間の中央値を縦軸にしたグラフを示す．伝搬時間の中央値は 100 ブロックごとに平均値をプロットした．

提案した隣接ノード選択アルゴリズムを採用することでネットワーク全体のブロック伝搬時間の中央値が改善されていることがわかる．最初の数十ブロックが生成されたことで起こる少ない回数の隣接ノードの張り替えで十分に伝搬時間が改善されていることもわかる．100 個のブロックが生成された以降は，伝搬時間のさらなる改善は見られない．本実験では提案アルゴリズムで全ノードからランダムに隣接ノードに選ぶ個数は 1 としていたが，その個数を変更することで，伝搬時間の改善の速さや限界などが変化する可能性がある．

4.3　リレーネットワーク

ブロックチェーンにおけるブロック伝搬時間の短縮を図る方法の一つとしてブロック配信用のリレーネットワークを構築することが提案されている．ブロックチェーンのブロック伝搬の仕組みは，悪意あるノードが存在する環境でも動作するが，伝搬効率に注目した場合は決して適なものではない．リレーネットワークはブロックチェーンの仕組みの外側に構築されたブロック伝搬用のネットワークであり，参加ノード間ではブロックチェーンの通常のブロック伝搬よりも早くブロックの送受信が可能である．

リレーネットワークでのブロック伝搬の効率化のための仕組みは実装により様々であるが，本実験ではその仕組みは抽象化した．リレーネットワークに参加しているノードは，リレーネットワークに参加している他のノード全体に通常の 10 倍の帯域幅を用いてブロックを送信できるものとした．リレーネットワークに参加しているノードの割合を変更しながら，ブロック伝搬時間の中央値を測定した．伝搬時間の中央値は，ブロックチェーンに参加しているノード全体，リレーネットワークに参加しているノード，リレーネットワークに非参加なノードの 3 種類のノード群での値を測定した．図 4 に 5000 ブロックの伝搬時間の中央値の平均をに示す．パラメータは 3. 章の Bitcoin と同様の条件で行った．

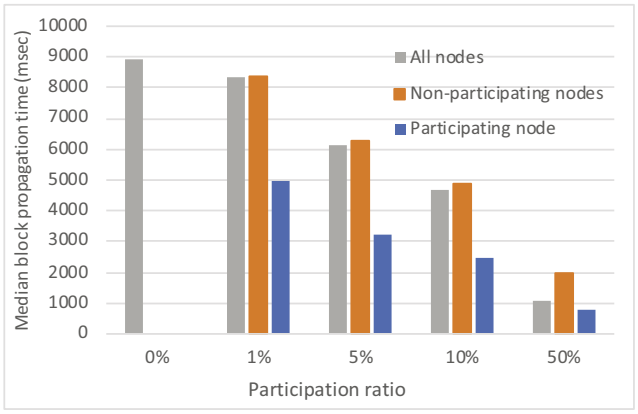

図 4　The median of block propagation time

リレーネットワークへの参加率が 5% と低い割合でも全体の伝搬時間は元々の 70% 以下と大きく改善されている．リレーネットワークに参加しているノード間の伝搬時間はさらに大きく改善されている．リレーネットワークへの参加率が大きくなるほど，非参加ノードと参加ノードとの伝搬効率の差が大きくなって行くことがわかる．

5.　まとめと課題

本提案ではブロックチェーンのシミュレータを提案した．シミュレータが実際のブロックチェーンを良い精度でシミュレートできていることを確認した．シミュレータの活用例を示し，シミュレータが研究において有用であることも示した．シュミレータは今後，実験シナリオの入力方法やデータの出力方法を整備したのちに Web サイトで公開する予定である．

今後の課題としては，シミュレータのさらなる拡張が挙げられる．現在のシミュレータはシンプルなブロック送信プロトコルをシミュレートしているが，コンパクトブロック等の最新の送信プロトコルにも対応した実装を追加したい．また今回行っていないトランザクションのシミュレートも追加したい．トランザクションの送受信等はブロックの送受信に用いた仕組みを一部使用して追加できると考えている．

シミュレータは入出力方法を整理した上で，数ヶ月後に Web 上で公開する予定である．

文　　献

[1] Satoshi Nakamoto. Bitcoin: A peer-to-peer electronic cash system. 2008.
[2] Bitcoin Core : Bitcoin. https://bitcoincore.org, (accessed Jan. 10, 2019).
[3] Andrew Miller, James Litton, Andrew Pachulski, Neal Gupta, Dave Levin, Neil Spring, and Bobby Bhattacharjee. Discovering bitcoin’s public topology and influential nodes. 2015.
[4] Arthur Gervais, Ghassan O Karame, Karl Wüst, Vasileios

Glykantzis, Hubert Ritzdorf, and Srdjan Capkun. On the security and performance of proof of work blockchains. In *Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security*, pp. 3–16. ACM, 2016.

[5] VisaNet | Electronic Payments Network. `https://usa.visa.com/about-visa/visanet.html`, (accessed Jan. 10, 2019).

[6] PayPal, Inc | PayPal Reports Second Quarter 2018 Results. https://investor.paypal-corp.com/news-releases/news-release-details/paypal-reports-second-quarter-2018-results?ReleaseID=1072972, (accessed Jan. 10, 2019).

[7] Christian Decker and Roger Wattenhofer. Information propagation in the bitcoin network. In *Peer-to-Peer Computing (P2P), 2013 IEEE Thirteenth International Conference on*, pp. 1–10. IEEE, 2013.

[8] Uri Klarman, Soumya Basu, Aleksandar Kuzmanovic, and Emin Gün Sirer. bloXroute: A scalable trustless blockchain distribution network whitepaper.

[9] Falcon - A Fast Bitcoin Backbone. https://www.falcon-net.org/, (accessed Jan. 10, 2019).