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
IA2022-19(2022-09)

ブロックチェーンネットワークにおける Plumtree 適用のシミュレーション評価

北川　雄介† 　首藤一幸 *†† 　水野　　修† 　坂野　遼平†

† 工学院大学　〒192-0015 東京都八王子市中野町 2665–1
†† 東京工業大学　〒152-8550 東京都目黒区大岡山 2–12–1

あらまし　ブロックチェーンでは，多数のノードがランダムに相互接続し，Peer-to-Peer ネットワークを形成しており，各ノードは，P2P ネットワーク内の他のすべてのノードに情報をブロードキャストを行う．これはフラッディング方式で行われ，情報を受け取ったノードはその情報を近隣のノードに転送する．そのため，既に受信した情報を異なる近隣ノードを通じて複数回受信する可能性があり，通信リソースの過剰な消費を招く．本研究では，効率的なブロードキャスト方式として知られる Plumtree アルゴリズムを用いて，Bitcoin ネットワークにおける通信リソース消費の問題を解決することを目指す．ブロックチェーンネットワークのシミュレータ SimBlock に Plumtree の Eager push, Lazy push 等の動作を組み込み，シミュレーションを行った．シミュレーション実験によって，提案手法では，ツリーの構築完了後，ツリー修復のメッセージを含めても従来手法と比べメッセージ数を削減可能であることが明らかとなった．
キーワード　ブロックチェーン，SimBlock，Plumtree，P2P ネットワーク

Simulation Evaluation of Plumtree Application in Blockchain Networks

Yusuke KITAGAWA†, Kazuyuki SHUDO*††, Osamu MIZUNO†, and Ryohei BANNO†

† Kogakuin University　2665–1 Nakano-machi, Hachioji-shi, Tokyo, 192–0015 Japan
†† Tokyo Institute of Technology　2–12–1 Ookayama, Meguro-ku, Tokyo, 152–8550 Japan

Abstract　In a blockchain, many nodes are randomly interconnected to form a peer-to-peer (P2P) network, and each node broadcasts information to all other nodes in the P2P network. This is done in a flooding fashion, where each node that receives information forwards it to its neighbors. Therefore, information that has already been received may be received multiple times through different neighbors, resulting in excessive consumption of communication resources. This research aims to solve the problem of communication resource consumption in Bitcoin networks by using the Plumtree algorithm, which is known as an efficient broadcast method. In this simulation experiment, we implemented Plumtree's Eager push, Lazy push, and other operations in SimBlock and performed simulations.Simulation experiments show that the proposed method can reduce the number of messages compared to the conventional method, even including tree repair messages after the completion of tree construction.
Key words　Blockchain, SimBlock, Plumtree, Peer-to-Peer network

1. はじめに

ブロックチェーンに代表される分散型台帳技術は，多数の参加者が記録を共有し，改ざんが困難な状態で保管するシステムである．Bitcoin [1] をはじめとする仮想通貨や金融サービスへの応用が知られており，経済産業省は，ブロックチェーンの日本での市場規模を約 67 兆円と推計している [2]．ブロックチェーンでは，多数のノードがランダムに相互接続し，P2P (Peer-to-Peer) ネットワークを形成しており，各ノードは，P2P ネットワーク内の他のすべてのノードに対し，情報をブロードキャストする．これはフラッディング方式で行われ，情報を受け取ったノードはその情報を近隣のノードに転送する．そのため，既に受信した情報を異なる近隣ノードを通じて複数回受信する可能性があり，通信リソースの過剰な消費を招く．本研究では，効率的なブロードキャスト方式として知られる Plumtree アルゴリズム [3] を用いて，Bitcoin ネットワークにおける通信リソース消費の問題を解決することを目指す．この論文は，電

（注）：∗ Present affiliation: Kyoto University
（注）：This is an unrefereed paper.

子情報通信学会 ICETC2021 で発表された研究 [4] の拡張版である．差分には，Plumtree のツリーの修復機能と最適化機能を実装し，それに対する追加の実験と関連する研究についての議論が含まれている．

2. ブロックチェーン

ブロックチェーンは，Satoshi Nakamoto と名乗る人物によって投稿された論文 [1] に基づいて実装された Bitcoin 及び仮想通貨の基盤技術である．ブロックチェーンは特定の第三者を介さずに，オープンなネットワークで参加者による分散の合意形成を可能にし，すべての履歴を追跡可能にして透明性の高い取引を実現する．その他の特徴として，データの改ざんが極めて困難，ゼロダウンタイムの実現といったものがあり，様々な分野で利用が期待されている．

2.1 ブロードキャスト

図 1 は，Bitcoin のネットワークでブロックがブロードキャストされるまでのシーケンスを示している．Bitcoin のノードはブロックを受信すると，まず近隣のノードに “inv” メッセージを送信する．メッセージを受け取ったノードは，欠落しているブロックがないかどうかを確認する．もし足りないブロックがあれば，inv メッセージの送信者ノードに “getdata” メッセージを送り，足りないブロックを送るよう依頼する．この仕組みにより，ブロックの重複配信を排除することができる．ブロックの重複配信は回避できるが，inv メッセージの重複配信の問題が残る．inv メッセージはフラッディング方式で伝搬されるため，あるノードが異なる隣接ノードを介して複数回受信する可能性がある．

3. 関 連 研 究

ブロックチェーンネットワークのネットワークの通信量を削減することを目的とした既存の研究がいくつか存在する．Kan らの研究 [5] では，ブロックチェーンネットワークに Tree-based の構造を導入する手法を提案している．冗長性を得るために，各ノードは配送ツリーを構成するノードグループに参加する．この方法は，Tree-based のルーティングの利点があるが，各メッセージがグループ内でフラッディング方式でグループメンバー間で共有されるため，依然として冗長な通信が発生する問題が存在する．Jin らの研究 [6] では，ブロック伝搬に消失訂正符号を用いる方法を提案している．この方式では，各ノードがブロックの全情報を送信する必要がない．これにより，ブロック伝搬に必要な帯域を削減することができるが，inv と getdata メッセージの交換は必要である．本研究では， Tree-based と Gossip-based を組み合わせた新たな手法を提案し，少ないメッセージ数と高い耐障害性の両立を狙う． Bitcoin における Gossip-based の P2P ネットワーク上に Tree-based を作成する．ブロードキャストは基本的に Tree-based 方式で転送する．また，Tree-based で利用していないリンクを用いて，ノード離脱等に，Gossip-based のリンク情報用いて確実な伝播を実現する．

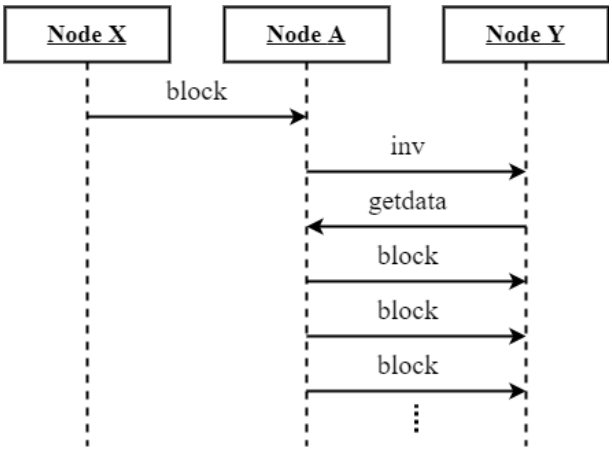

図 1　Bitcoin のメッセージのシーケンス

4. 提 案 手 法

既に受信したメッセージが異なるノードを経由して複数回配信されるという問題がある．本研究では，Bitcoin ネットワークをベースに Plumtree [3] の冗長なメッセージ送信を削減する機能を用いて，通信リソースの過剰消費問題を解決する．

4.1 Plumtree

Plumtree [3] は Tree-based と Gossip-based を組み合わせたブロードキャスト方式で，メッセージの信頼性を高く保ちつつ冗長性を低減することができる．この方式では，各ノードは基本的に Tree-based 方式でメッセージ転送を行う．また，ネットワーク障害を適切に処理するために，Gossip-based 方式を使用する．

4.1.1 Tree-based と Gossip-based

Plumtree は，Gossip-based のアプローチに基づいて設計されている．このアプローチの基本は，すべてのノードがメッセージの伝搬に等しく貢献することである．この目的を達成するために，ノードがメッセージをブロードキャストするとき，メッセージを送信するノードをランダムに選択する．初めてメッセージを受信した各ノードは，このプロセスを繰り返す．この性質により，ネットワークの障害やノード数の増減に柔軟に対応することができる．Gossip-based では，図 2 のように以下のアプローチを使用する．

- Eager push : メッセージを受信すると，すぐに近隣のノードに送信する．
- Lazy push : ノードはメッセージを受信すると，メッセージの識別子を隣接するノードに送信する．識別子を受け取ったノードがメッセージを受信していない場合，Pull リクエストを行う．

Plumtree は Eager push と Lazy push の仕組みを組み合わせて，それぞれ少数のメッセージを送信して支援する．

4.1.2 ツリーの最適化

ブロードキャストを開始するノードは，eagerPushPeers に含まれる全隣接ノードにメッセージを送信する．メッセージを受信した各ノードも，同様に，eagerPushPeers に含まれる全隣

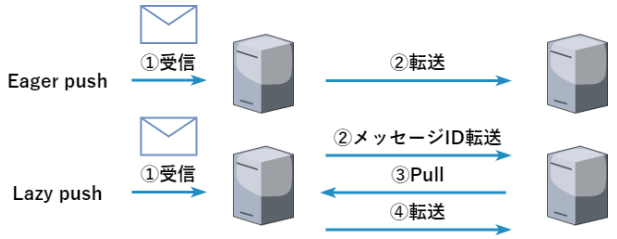

図 2　Gossip-based のやり取り

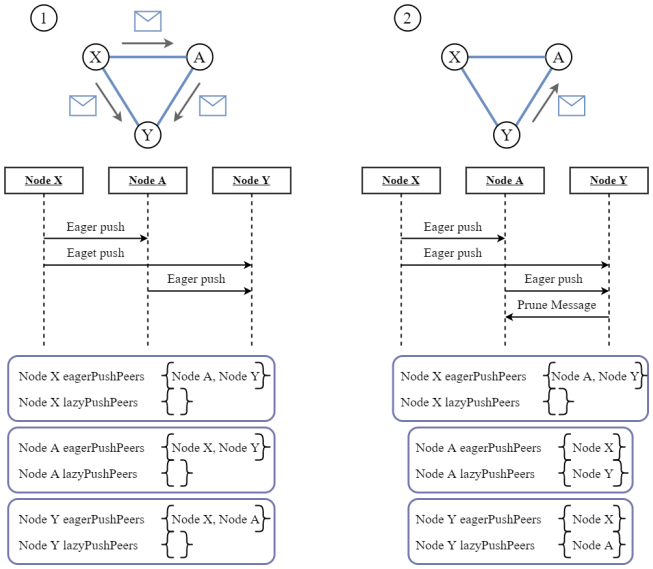

図 3　PRUNE メッセージ

接ノードにメッセージを送信する．初期状態では，各ノードの eagerPushPeers には全隣接ノードが入っているため，最初のブロードキャストは，通常の Gossip-based と同じになる．受信したメッセージが，初めて受信するものであった場合，送信元ノードを eagerPushPeers に追加する．もし受信したメッセージが，受信済みのものであった場合，送信元ノードを eagerPushPeers から lazyPushPeers へと移す．そして，図 3 のように，送信元ノードに PRUNE メッセージを送る．PRUNE メッセージを受信したノードは，PRUNE メッセージの送信元ノードを eagerPushPeers から lazyPushPeers へと移す．このように，PRUNE メッセージを利用して，経路を最適化していく流れとなっている．

4.1.3　ツリーの修復

Eager push に加え，各ノードは Lazy push も行う．障害が発生すると，Eager push では全てのノードに行き届かなくなる．Lazy push は，そのような場合にメッセージを未受信ノードへと届ける役割と，ツリーを修復する役割とを担う．Lazy push は，図 4 のように lazyPushPeers に含まれる各隣接ノードに対して，定期的に IHAVE メッセージを送信する．IHAVE メッセージにはメッセージ ID を載せてあり，定期送信の間隔を大きくすることで，通信量を削減することができる．定期送信の間隔により，1 回の通信で複数の IHAVE メッセージをまとめて送る．IHAVE メッセージを受信したノードは，当該メッセージをまだ Eager push で受け取っていない場合，そのメッセージを missing として一定時間待機する．待機時間が経過するまでに

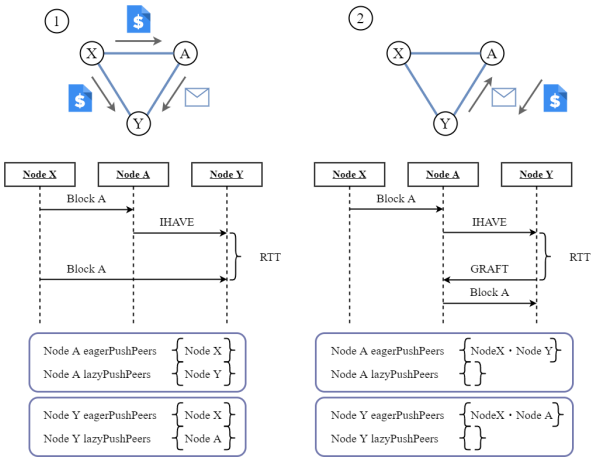

図 4　IHAVE・GRAFT メッセージ

Eager push で当該メッセージが届いた場合は，ツリー修復は行わない．もし待機時間が経過するまでに Eager push で当該メッセージが届かなかった場合，以下の処理を行う．

- 該当する IHAVE メッセージを最初に送ってきたノードを lazyPushPeers から eagerPushPeers に移す．そして，ノード A に GRAFT メッセージを送信する．
- ノード A は GRAFT メッセージを受信したら，ノード Y を lazyPushPeers から eagerPushPeers に移す．そして，該当するメッセージをノード Y に転送する．

4.2　スパニングツリーの構築

提案手法では，Plumtree を Bitcoin ネットワークに適用する．最初は，図 1 に示すように，Bitcoin の標準的な手順でブロックがブロードキャストされる．その際に使用した経路情報を元に，各ノードにスパニングツリーにおける隣接関係の情報を付与していく．各ノードが持つ情報を以下に示す．

- eagerPushPeers : スパニングツリーにおける隣接するノード集合
- lazyPushPeers : スパニングツリーにおける eagerPushPeers 以外の隣接するノード集合

最初のブロードキャストでは，Plumtree アルゴリズムに従ってスパニングツリーが構築される．その後のブロードキャストでは，構築されたツリーが使用される．図 6 のように，ノード間の inv や getdata メッセージのやり取りを省略し，ツリーの子ノードへ直接ブロックを送信している．また，ノードの切り替わりやネットワーク障害に対しては，Plumtree の Gossip ベースの修復処理を用いている．

図 5 を用いて，Plmutree の動作を説明する．eagerPushPeers の情報を持つ全てのノードは Eager push によりメッセージを送信する．重複したメッセージを受信した場合，そのノードは lazyPushPeers のリストに追加される．最初のブロードキャストが完了すると，スパニングツリーが形成される．安定したネットワークでは，スパニングツリー上の Eager push によってのみブロードキャストが可能である．もし C のノードが離脱してメッセージを送ることができなくなった場合，そのノードは新しいメッセージを受け取ったかどうかわからないので，その

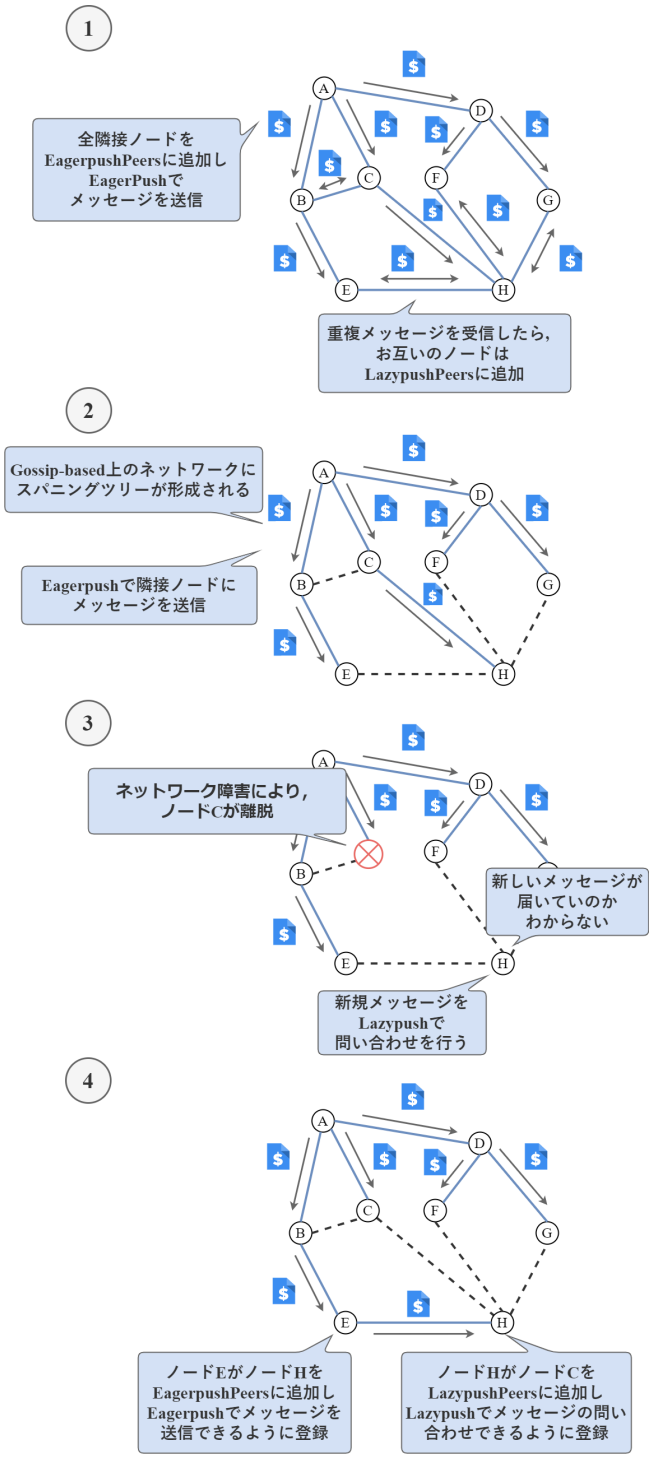

図 5　Plumtree の動作

ノードに含まれる lazyPushPeers に Lazy push で新しいメッセージを問い合わせを行う．このように，スパニングツリーを構築するために Plumtree アルゴリズムが使用される．

5. 評　　価

ブロックチェーンの情報伝搬を模擬できる SimBlock [7] を用いて，メッセージ数とホップ数の計測を行った．実験環境と評価結果について説明する．

5.1 SimBlock

SimBlock [7] は，インターネット上の多数のノード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ある．SimBlock は，実際に使用されているブロックチェーンのネットワークを再現しており，限りなく本物に近い環境でブロックチェーンの挙動を検証できるため，ブロックチェーンのネットワークを構成するノードの挙動を変更したり，新しい技術がネットワークにどのような影響を与えるかを検証することが可能である．

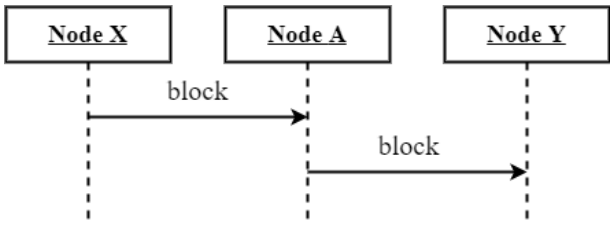

図 6　提案手法のメッセージのシーケンス

表 1　SimBlock パラメータ

パラメータ	内容
NUM_OF_NODES	100
BLOCK_SIZE	535 Kbyte
NUM_OF_RATE	100%
BLOCK_OF_RATE	3
CBR_USAGE_RATE	0
CHURN_NODE_RATE	0

5.2 測 定 環 境

本実験で使用した SimBlock の実験パラメータを表 1 に示す．Bitcoin の転送方式と Plumtree 適用時の転送方式の比較を行った．ネットワークに対する影響を調査するために，評価指標として 50% ブロック伝播時間を用いた．この変数は，研究 [8] で用いられており，影響を調査するうえで適切な評価指標であるといえる．ノードの増減はなしとし，CBR（Compact Block Realy) は利用せず，ブロックの伝播を 50 ブロックまでシミュレートを行った．それ以外は SimBlock のデフォルト値を利用している．試行回数は，10 回とした．

5.3 メッセージ数の評価

ブロックチェーンに Plumtree を適用した場合のメッセージ数の評価を行った．図 7 に，提案手法と従来手法のメッセージ数の比較を示す．縦軸は，全ノードの受信メッセージ数の合計，横軸はブロック数である．この提案手法のメッセージ数は，初回ブロードキャスト時のみ inv メッセージが生じる．2 回目は，Eager push で受信したメッセージが，受信済みのものであった場合，送信元ノードに PRUNE メッセージを送信し経路情報を更新するため，メッセージ数が多くなる．そして，3 回目以降では Plumtree で作成されたスパニングツリーを用いるため，inv メッセージのやり取りは不要となっている．結果，従来手法よりもメッセージ数が少なくなっている．安定したネットワークであれば，IHAVE メッセージの送信頻度を下げることで，よりメッセージ数を削減することが可能である．

5.4 ホップ数の推移

ブロックごとのホップ数の推移を計測を行った．図 8 に，提

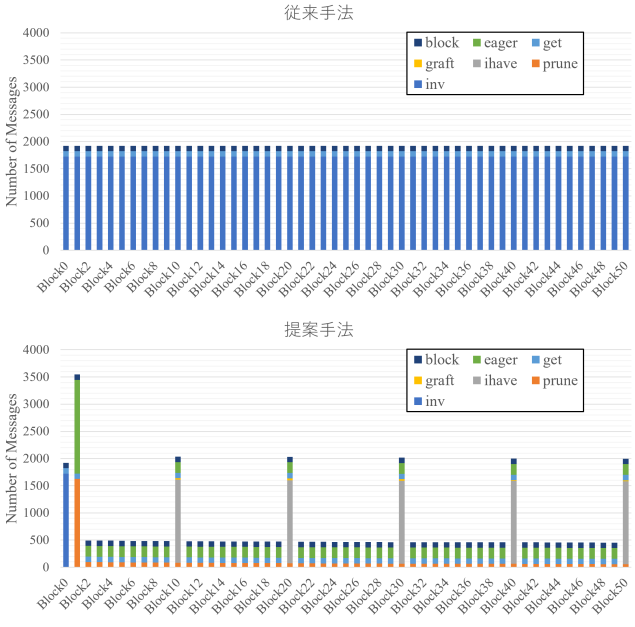

図 7　提案手法と従来手法のメッセージ数

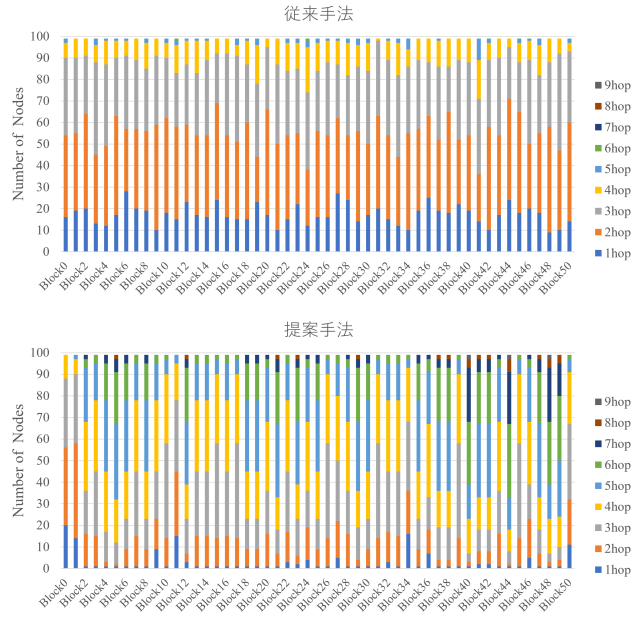

図 8　提案手法と従来手法におけるホップ数の推移

案手法と従来手法のホップ数の推移を示す．縦軸は，ノード数，横軸はブロック数である．従来手法の方では，ブロックごとに自身の近隣ノードに対し，inv メッセージを送信しメッセージの共有を行うため，ホップ数は 1 や 2 とかなり近い場所のノードに対して，送信を行えている．一方で提案手法では，最初のブロックを送るノードに合わせて経路を構築するため，それ以降のブロックが構築したスパニングツリーの根から遠い，他のノードにより送信されると，最短ではない経路を用いて転送されるため，ホップ数が増加してしまう．

5.5　ブロック伝播時間

Plumtree により，ホップ数が増加してしまうことから，ブロックの伝播時間に影響があるかを確認を行った．図 9 は，ネッ

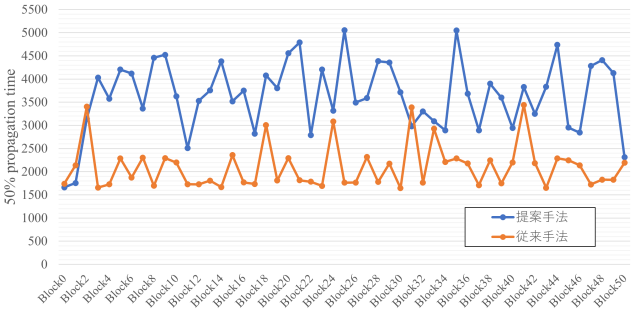

図 9　50% ブロック伝播時間

トワーク全体の 50% ブロック伝搬時間を図示している．従来手法では，自身の近隣ノードに対し通信を行っているため，ブロックの伝播時間が比較的に安定して，ブロックの送信をしていることがわかる．提案手法の方では，最初のブロックを送るノードに合わせて経路を構築するため，最初のブロックの伝播時間は，提案手法と同様の時間で送信を行えているが，ホップ数の推移が多くなるほど，ブロックの伝播時間が多く掛かってしまう．

6.　ま　と　め

本研究では，ブロックチェーンネットワークにおけるメッセージ削減手法を提案し，シミュレーションによる評価を行った．その結果，Plumtree アルゴリズムを適用することで，従来手法と比較してメッセージ数が削減されることが分かった．また，Plumtree の最適化処理により，無駄なメッセージ送信が無くなったが，ブロックの送信元が作成されたツリーの根から遠いほど，伝播時間及びホップ数の推移が増加することを確認した．今後は，スパニングツリーの構築を改善し，ホップ数及び，伝搬遅延を削減する手法を検討する予定である．

謝辞 本研究の一部は，日揮・実吉奨学会の支援を受けて行われたものである．本研究の一部は，JSPS 科研費 21H04872 の支援を受けて行われたものである．

文　　献

[1] S. Nakamoto, “Bitcoin: A peer-to-peer electronic cash system,” `https://bitcoin.org/bitcoin.pdf` (accessed Aug. 24, 2022), 2008.

[2] Ministry of Economy, Trade and Industry (METI), “Fy2015 survey report on the infrastructure development for the informatization and servitization of japan’s economy and society,” `https://www.meti.go.jp/main/infographic/pdf/block_c.pdf` (accessed Aug. 24, 2022), 2015.

[3] J.a. Leitão, J.P. Luěıs, and Rodrigues, “Epidemic broadcast trees,” 2007 26th IEEE International Symposium on Reliable Distributed Systems (SRDS 2007), pp.301–310, 2007.

[4] Y. Kitagawa, K. Shudo, O. Mizuno, and R. Banno, “Verification of applying plumtree algorithm for blockchain networks,” IEICE International Conference on Emerging Technologies for Communications (ICETC), 2021.

[5] J. Kan, L. Zou, B. Liu, and X. Huang, “Boost blockchain broadcast propagation with tree routing,” Smart Blockchain, ed. by M. Qiu, pp.77–85, Springer International Publishing, Cham, 2018.

[6] M. Jin, X. Chen, and S.-J. Lin, “Reducing the bandwidth of block propagation in bitcoin network with erasure coding,” IEEE Access, vol.7, pp.175606–175613, 2019.

[7] Y. Aoki, K. Otsuki, T. Kaneko, R. Banno, and K. Shudo, “Simblock: A blockchain network simulator,” IEEE INFOCOM 2019 - IEEE Conference on Computer Communications Workshops (INFOCOM WKSHPS), pp.325–329, 2019.
[8] K. Otsuki, K. Shudo, and R. Banno, “Effects of relay networks in bitcoin,” IEICE Tech. Rep., vol.119, pp.89–94, NS2019-192, 2020.