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
IA2021-7,ICSS2021-7(2021-06)

ブロックチェーンネットワークにおける Plumtree アルゴリズムの適用検証

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　暗号通貨を支える技術としてブロックチェーンが注目を集めている．ブロックチェーンは取引などを記録するための台帳をネットワーク上の複数のコンピュータで共有し改ざん困難な状態で保持する仕組みである．しかし，ブロックチェーンを活用する上で問題となるのが通信リソースの消費である．ブロックチェーンは全ノードに情報を行き渡らせるために各ノードが隣接するノードに対して情報を送信する．既に受信した情報が別ノード経由で複数回届くことで、通信リソースの過剰な消費が生じる場合がある．本研究では，ランダムなトポロジを持つブロックチェーンネットワークにおいて Plumtree アルゴリズムを適用することで伝播経路を緩やかに固定し，重複メッセージを削減する手法を提案する．シミュレーション実験によって，提案手法と既存手法の比較を行い，ブロック伝播を 4 ブロックまでシミュレートした場合には、メッセージ数を 75 %以上削減可能であることを確認した．

キーワード　ブロックチェーン，SimBlock，Plumtree，P2P ネットワーク

Verification of Applying Plumtree Algorithm to 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　Blockchain is gaining attention as a technology to support cryptocurrency. It is a system that prevents internal and external tampering by sharing a ledger for recording transactions among multiple computers on a network. However, one of the problems in using blockchain is the consumption of communication resources. It is caused by that the information received by a node can be delivered to the same node more than once through different neighbors. In this paper, we propose a method to reduce the number of duplicate messages in a blockchain network with random topology by applying an algorithm called Plumtree to fix the propagation path loosely. Through simulation experiments, we compared the proposed method with existing methods and confirmed that the number of messages can be reduced by more than 75 % when block propagation is simulated up to four blocks.

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台帳技術は、多数の参加者が記録を共有し、改ざん困難な状態で保持する仕組みである．Bitcoin [1] をはじめとする仮想通貨や金融サービスでの応用で知られており，そのトラストレスな性質から，IoT やデジタルサービスといった分野での運用に期待を集めており、経済産業省では、ブロックチェーンの国内市場規模をおよそ 67 兆円と予想している [2]．しかし，ブロックチェーンを活用していく上で大きな問題となるのが，通信リソースの過剰な消費である．Bitcoin をはじめとする典型的な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を行い，P2P ネットワークを形成する．各ノードは、全ノードに情報を行き渡らせるために，各ノードが隣接するノードに対して情報を送信する．情報を受信したノードもその情報を別のノードへ送信することを繰り返すことにより，情報を行き渡らせている [3]．そのため，既に受信した情報が別ノード経由で複数回届く場合があり，通信リソースの過剰な消費が生じる．

本研究では，Bitcoin ネットワークをベースに，効率的なブロードキャスト手法として知られる Plumtree アルゴリズム [4] を用いて通信リソースの消費問題を解決することを目的とする．

本稿の構成は以下の通りである．2 章ではブロックチェーン

について述べ，3 章では提案手法の詳細を述べる．4 章で評価実験の内容とその結果を述べ，最後に 5 章で本研究の今後の課題とまとめについて述べる．

2. ブロックチェーン

本章では，提案手法に関連するブロックチェーンについて述べる．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 ブロックチェーンの種類

ブロックチェーンネットワークには，オープンなネットワークで，誰でも自由に参加可能なパブリック型と，ネットワークへの参加に許可が必要なプライベート型，コンソーシアム型が存在する．それぞれのブロックチェーンネットワークの特徴を以下に示す．

- パブリック型ブロックチェーンネットワーク

管理者が存在せず，インターネットに接続可能であれば，誰でもノードとなり，ネットワークに参加することができる．

- プライベート型ブロックチェーンネットワーク

パブリック型ブロックチェーンとは異なり，単独の管理者が存在し，ノードとしてネットワークに参加するには，管理者による許可が必要とされる．

- コンソーシアム型ブロックチェーンネットワーク

特定かつ複数の管理主体がブロックの生成や承認を行うブロックチェーンを指し，パブリック型ブロックチェーンの分散性とプライベート型ブロックチェーンの迅速性の双方を兼ね備えている．しかし，特定の管理主体を信頼しなければならないというデメリットがあり，ブロックチェーンが本来持つ取引の透明性が失われる．

本論文ではパブリック型に着目する．

2.2 ブロードキャスト

Bitcoin のブロックの共有方法を図 1 の Bitcoin のメッセージのシーケンス図を用いて説明する．Bitcoin のブロックチェーンは，ノード同士でブロックを共有する際に，まず inv メッセージを送信する．受け取ったノードは，足りないブロックがあるか確認を行う．もし，不足しているブロックがある場合，inv メッセージの送信元ノードに，getdata メッセージを送信し，不足ブロックを送信してもらう．この仕組みにより，常にブロックをネットワーク全体に送信することがなくなり，余分な送信を減らしている．

3. 提 案 手 法

今後ブロックチェーンを活用していく上で問題が存在する．それは，通信リソースの消費である．ブロックチェーンネットワークでは，受信したメッセージを別のノードにも伝播して

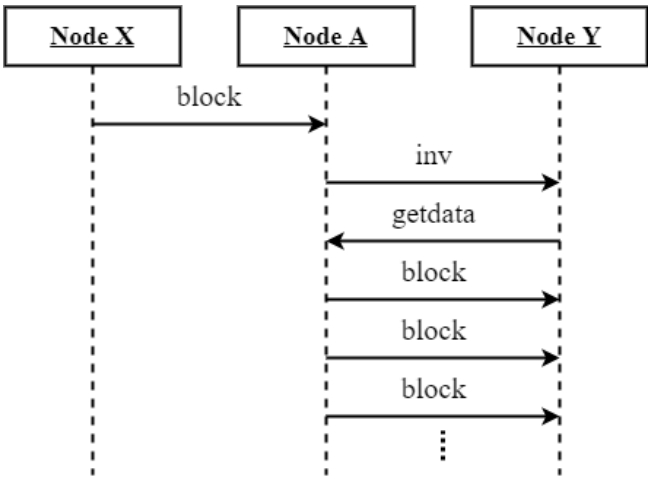

図 1　Bitcoin のメッセージのシーケンス図

メッセージを行き渡らせている．そのため，既に受信したメッセージが別ノード経由で複数回届くといった問題が存在する．これにより，通信リソースが過剰に消費されてしまう．Bitcoin においては前述の仕組みによりブロックの無駄な転送が低減されているが，inv メッセージが通信リソースを消費する問題がある．また，inv メッセージによる確認を要することから，伝播遅延が大きくなることも懸念される．

本研究では，Bitcoin ネットワークをベースに，Plumtree 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消費問題を解決する．

3.1 Plumtree

Plumtree は，メッセージの信頼性を高く保ちつつ冗長性を減らすために，Tree-based と Gossip-based を組み合わせたアプローチである．この手法は，メッセージの送信を Tree-based で行うが，Gossip-based のノード間のリンクを利用して，ノード間の障害にも適切に対処できるようになっている．

Plumtree は，効率的にメッセージの配送を行える特徴がある．これはランダムなネットワークにスパニングツリーを構築し，Tree-based でのみメッセージが転送されるようにすることで，冗長な送信を減らし，効率化しているためである．

Tree-based のブロードキャストでは，ネットワークに全域木を構築し，Tree でのみメッセージが送信されるようにすることで，メッセージの冗長性が低くなる．しかし，ノードの増減やネットワーク障害が発生した場合に，全域木が形成されていない状態となり，メッセージが全ノードに届かない可能性がある．Gossip-based のブロードキャストでは，あるノードがメッセージをブロードキャストした場合，ノードはメッセージを送信するノードをランダムに t 個選ぶ．初めてメッセージを受信したノードはこの処理を繰り返しメッセージの送信をすることで，高いスケーラビリティを提供するだけでなく，ネットワークの不備やノードの障害に強くなっている．しかし，冗長性が高くなる傾向がある．

3.1.1 Plumtree の動作

Plumtree は, メッセージをブロードキャストするために Gossip-based を軸に設計されている．Gossip-based は，すべてのノー

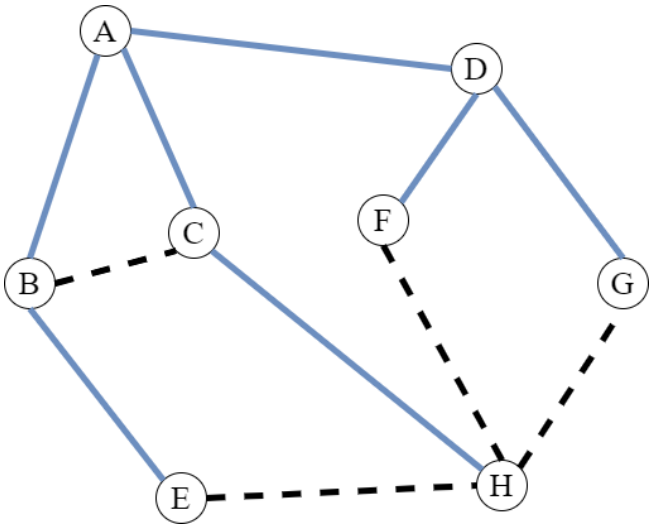

図 2　スパニングツリーの例

ドがメッセージの伝播に平等に貢献するという考え方に基づいている．この考え方を達成するために，あるノードがメッセージをブロードキャストする場合，ノードは送信するノードをランダムに選ぶ．初めて受信したノードはこの処理を繰り返していく．この性質により，ネットワーク障害やノードの増減に対して柔軟に対応できるようになっている．

Gossip-based では以下のアプローチを使用する．

- Eager push アプローチ

メッセージを受信するとすぐに，隣接するノードにメッセージを送信する．

- Lazy push アプローチ

ノードがメッセージを受信すると，隣接するノードにメッセージ識別子を送信する．ノードがメッセージを受信していない場合，ノードは Pull リクエストを行う．

- Pull アプローチ

定期的に，ノードは隣接するノードに最近受信したメッセージに関する情報を問い合わせる．

Plumtree では，Eager push の少ないメッセージ数で送る仕組みと，Lazy push の送信補助の仕組みを組み合わせた手法を利用している．

3.2　スパニングツリーの構築

提案手法は，まず Bitcoin と同じ仕組みでブロックをブロードキャストする．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

例えば，図 2 より，ノード B の eagerPushPeers はノード A とノード E であり，lazyPushPeers はノード C である．

基本の動作としては, eagerPushPeers の情報を持つ全ノードは, Eager push でメッセージを送信する．定期的に，lazyPushPeers

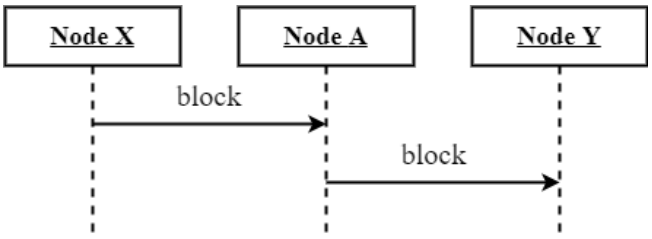

図 3　提案手法によるメッセージのシーケンス図

に含まれるノードに，識別子を送信し最近受信したメッセージに関する情報を問い合わせる．受け取ったノードは，メッセージを受信していない場合，Lazy push でメッセージの送信をリクエストする．この Plumtree のアルゴリズムを用いてスパニングツリーを構築する．

それ以降のブロードキャストでは，構築したツリーを利用する．その際，メッセージの送信は図 3 のように，inv・getdata メッセージのやり取りは省き，ツリーの子ノードに直接ブロックを送る．ノードの増減やネットワーク障害に伴って必要となるツリー修復については，Lazy push アプローチ及び pull アプローチを利用して修復を行う．

4.　評　　価

ブロックチェーンの情報伝播を模擬できる SimBlock を基に，メッセージ数とホップ数の測定を行った．本実験で構築したシステム及び，プログラムについて説明する．まず，本実験で使用したシミュレータ SimBlock について説明する．

4.1　SimBlock

SimBlock 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 [5]. 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る．これにより，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る．また，SimBlock は実際に使われているブロックチェーンのネットワークを再現しているため，本物に近い挙動を調べることができるようになっている．

4.2　システム・プログラム概要

Plumtree の実装に関しては，あるノードが最初のブロックをブロードキャストする際，隣接するノードにブロックを送信したときの情報を利用して，子ノード集合の配列を作成した．この子ノード集合の配列には，ブロックの送信が完了したタイミングでノードの情報を格納するようにプログラムし，次のブロックのブロードキャストから，その子ノード集合の配列を利用して，最初に格納されたノードから送信するように設定した．

次に inv・getdeata メッセージのカウントに関しては，プログラム上で inv メッセージと getdata メッセージの数をカウントするプログラムを実装して，全ノードの受信メッセージ数の合計を算出した．

表 1　SimBlock パラメータ

パラメータ	内容
NUM_OF_NODES	8370
BLOCK_SIZE	803.565 Kbyte
CBR_USAGE_RATE	0
CHURN_NODE_RATE	0

表 2　Plumtree 適用前と後のメッセージ数

メッセージ	メッセージ数
inv(提案手法)	144714
inv(既存手法)	578856
getdata(提案手法)	144714
getdata(既存手法)	578856

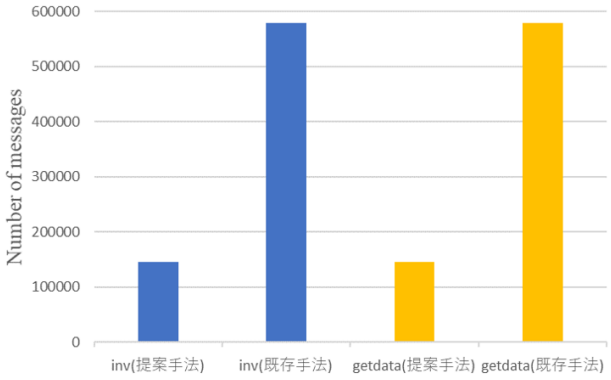

図 4　Bitcoin の inv・getdata メッセージ数

4.3　実 験 設 定

本実験で使用した SimBlock の実験パラメータを表 1 に示す．Bitcoin のチャート情報より，参照したデータは，ノード数は 8370，ブロックサイズは 803.565Kbyte に設定した [6]．これらは，2020 年 12 月 15 日時点の値である．ノードの増減はなしとした．CBR（Compact Block Realy) は利用せず，ブロックの伝播を 4 ブロックまでシミュレートをし，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．

4.4　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．表 2 に，Bitcoin のブロックチェーンにおける提案手法と従来手法のメッセージ数を示す．また，図 4 に，Bitcoin の提案手法と従来手法のメッセージ数の比較の図を示す．縦軸は，全ノードの受信メッセージ数の合計，横軸は測定項目である．Bitcoin の提案手法と既存手法を比べると 75 %以上のメッセージ数の削減が行えていることがわかった．

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 メッセージや getdata メッセージが生じる．2 回目以降は Plumtree で作成されたスパニングツリーを用いるため，これらメッセージのやり取りは不要となっている．結果，既存手法よりもメッセージ数が少なくなっている．

4.5　ホップ数と遅延時間の関係

ブロックチェーンに Plumtree を適用した場合のホップ数と遅延時間の関係を調査した。図 5 に提案手法のホップ数と遅延時

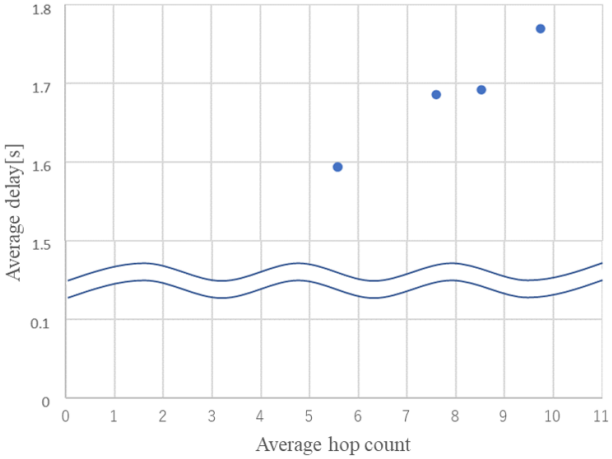

図 5　Bitcoin のホップ数と遅延時間の関係

間の関係を示している．縦軸は，1 ブロック当たりの平均遅延，横軸は平均ホップ数である．提案手法を見ると、平均ホップ数が多いほど、平均遅延も上がるようになっている．ホップ数が多くなる理由としては，Plumtree により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ことが挙げられる．またホップ数が多いほどブロックが届くまでの時間が長くなり，伝播遅延が増大することが予想される．

5.　お わ り に

本研究によりメッセージ数の削減を見込めることが明らかとなったが，Plumtree の適用によって，ホップ数が多くなりやすい傾向にある．今後の課題として，ホップ数を削減するためにスパニングツリーの構築を改良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] Satoshi Nakamoto, "Bitcoin: A Peer-to-Peer Electronic Cash System", 2008.
[2] 経済産業省, "平成 27 年度我が国経済社会の情報化・サービス化に係る基盤整備（電子商取引に関する市場調査）調査報告書" August 8, 2016
[3] Andreas M. Antonopoulos 著, 今井崇也, 鳩貝純一郎訳“ビットコインとブロックチェーン 暗号通貨を支える技術”, NTT 出版, 2016.
[4] João Leitão, Jos Pereira, Luĕıs Rodrigues, "Epidemic Broadcast Trees", 26th IEEE International Symposium on Reliable Distributed Systems (SRDS 2007), pp.301-310, Oct. 2007.
[5] Yusuke Aoki, Kai Otsuki, Takeshi Kaneko, Ryohei Banno, Kazuyuki Shudo, "SimBlock: A Blockchain Network Simulator", Workshop on Cryptocurrencies and Blockchains for Distributed Systems (CryBlock, in conjunction with IEEE INFOCOM), pp. 325-329, April 2019.
[6] BitInfoCharts, https://bitinfocharts.com (Accessed December 15, 2020)