ブロックチェーンネットワークの効率化と安定化のためのノード再接続方式の提案

M2018SE005 石塚 雄太
指導教員：沢田 篤史

1 はじめに

ブロックチェーンシステムを動作させるために必要なブロックチェーンネットワークには，安定した動作が求められる．近年，ブロックチェーンシステムは暗号通貨以外の領域での活用が検討されている．銀行業務や決済への適応，ヘルスケア分野や製造業をはじめ，農業や自動運転などさまざまな産業分野への適用がなされている [1]．

隣接ノードをランダムに選択してブロックチェーンネットワークに接続する方法では，伝搬遅延が生じる可能性がある．接続先のノードが P2P ネットワークに参加または離脱する頻度が高い，すなわちチャーン率が高い場合や，物理ネットワークからみて不安定である場合には，通信が途切れやすいのでメッセージの伝搬が遅延する．伝搬遅延が起こると，トランザクションやブロックの送受信を効率よく行うことができなくなる．

ブロックチェーンネットワークでは，伝搬遅延が生じるとフォークが発生する．フォークが発生すると，各ノード間で異なるブロックを最新のブロックと見なすので，データの整合性が取れなくなる．フォークの発生率が高いと，セルフィッシュ·マイニング攻撃などの攻撃に弱く，セキュリティ上の大きなリスクとなる．

本研究の目的は，ブロックチェーンネットワークにおけるメッセージの伝搬効率と安定性を改善する手法を提案することである．この目的を達成するために，青木らの研究 [4] や Bi らの研究の提案手法 [3] を改良する．それらの既存研究では通信の安定性について考慮されていないので，チャーン率の低いノードを隣接ノードに選択できるように評価指標を追加する．

提案手法を用いることで，ブロックチェーンネットワークにおいて効率よくかつ安定した通信が行うことが可能になる．提案手法を用いれば，ブロックチェーンノードが P2P ネットワークに参加する際，チャーン率の低いノードを隣接ノードに選択することが可能になる．チャーン率の低いノードは通信が途切れにくいので，結果としてトランザクションやブロックの伝搬を効率的に行うことができる．

2 ブロックチェーンにおける伝搬効率に関する課題

2.1 ブロックチェーン技術

P2P ネットワークに任意のノードが参加可能なパブリック型ブロックチェーンでは，ノードが P2P ネットワークに接続するとき，接続先のノードはランダムに選択される．ブロックチェーンネットワークにおいて，ノードが新たな隣接ノードと接続するとき，P2P ネットワーク全体で大まかに共有されている参加ノードのリストから宛先ノードを選択する．ブロックチェーンネットワークに参加しているノードは，自身が保持するノード情報を交換する．新しい隣接ノードが必要になると，このノード情報を使用して新たな隣接ノードを選択する．ブロックチェーンノードが P2P ネットワークを離脱後，P2P ネットワークに再参加する際にも同様の手続きをする．これを，P2P ネットワークに再接続するという．

パブリック型ブロックチェーンにおいて，メッセージはすべての隣接ノードへブロードキャストされる．ブロードキャストとは，トランザクションやブロックをブロックチェーンネットワークに送信し，全参加者に伝搬させることである．ネットワークに新しく参加したノードは，1 つまたはそれ以上の接続を確立すると，自身の IP アドレスが含まれた情報を隣接ノードに送信する．隣接ノードは，それをさらに隣接するノードに転送し，新しく接続されたノードがネットワーク上でよく知られた存在になるようにする．新しく接続されたノードは，隣接ノードから他のノードの IP アドレスリストを得ることができる．これにより，ノードは接続するノードを新たに見つけることができるので，その存在を他のノードに知らせることができる．

シャーディングとは，ブロックチェーンネットワーク上のノードをシャードと呼ばれる単位に分割し，各シャードごとにブロックの生成やブロックの検証作業を分割して並列実行させるための技術である．ノードをいくつかのシャードに分けて，ネットワーク全体で実施する処理を分割することで，スループットの向上を図っている．

2.2 ブロックチェーン伝搬効率に関する課題

パブリック型ブロックチェーンにおいて，接続先のノードがランダムに選択される方法には問題がある．P2P ネットワークに参加するためには，ネットワークにすでに存在するノードと接続する必要がある．ランダムに接続された隣接ノードのチャーン率が高かったり，物理的に距離が離れているノードである場合，隣接ノードとの通信において伝搬遅延が生じる．

P2P ネットワークにおけるノードの頻繁な参加・離脱のことをチャーンと呼ぶ．チャーン率の高いノードは通信が途切れやすい傾向にあるので [2]，接続先の隣接ノードのチャーン率が高い場合，伝搬遅延が生じる可能性が高い．

ブロックチェーンノードがモバイル端末である場合など，物理トポロジが頻繁に変化する状況では，下位レイヤとの不整合が生じる．ブロックチェーンネットワークにあるノードの IP アドレスが変化すると，物理ネットワークのトポロジも変化するので，頻繁に IP アドレスが変化

するにおいては、メッセージを伝播する経路が長くなる場合がある．

ネットワークで伝搬遅延が生じると，フォークの発生率が高くなる．フォークとは，２つの異なるブロックがネットワークを介して伝搬され，ブロックチェーンが分岐している状況のことである．フォークが発生すると，各ノード間で異なるブロックを最新のブロックとしてみなすことになるので，データの整合性が一時的にとれない．フォークの発生率が高いと，セルフィッシュ・マイニングなどの攻撃に弱く，セキュリティ上の大きな欠陥となる．これらの課題は，シャーディング技術においても同様に起こりうる．

2.3 関連研究

青木らの研究 [4] では，ブロック伝搬時間が短い P2P ネットワークを形成するための隣接ノード選択アルゴリズムを提案している．トランザクションの承認時間の長さとスループットの短さを問題として挙げ，ブロック生成間隔を短縮するだけでなく，あわせてブロック伝播時間を短縮することで解決できるとした．

Bi らの研究 [3] は，IP 層以下のネットワークの情報を用いて P2P ネットワークを形成する手法を提案している．Bitcoin や Ethereum で用いられるランダムな隣接ノードへの接続方法におけるメッセージの遅延が発生する問題を解消するために，RTT(Round Trip Time:往復通信にかかる時間) 測定によって隣接ノードをレイテンシの低い順に更新する方法を提案した．

3 ノードの再接続を考慮した隣接ノード選択方法の提案

3.1 提案手法の概要

本研究では，パブリック型ブロックチェーンにおけるメッセージの伝搬効率と通信の安定性を改善するための手法を提案する．青木らの研究 [4] や Bi らの研究 [3] などの既存研究では，通信の安定性について考慮されていないので，チャーン率の低いノードを隣接ノードに選択できるように評価指標を追加する．チャーン率が低いノードは，チャーン率が高いノードと比較して P2P ネットワークに長時間接続していると考えられるので，メッセージ通信が途切れる可能性を低くでき，伝搬遅延の発生を抑えることができる．

隣接ノードを選択する際に利用する指標には，ブロックチェーンネットワークにおけるメッセージ送信の速度，レイテンシ，チャーン回数の 3 つを用いる．メッセージ送信の速度は，ブロックを生成した時刻からブロックを受信した時刻の差分で測定する．レイテンシについては，物理ネットワークにおける応答時間を用いることで測定する．チャーン回数は，ICMP ECHO により下位ネットワークの接続状態から計測する．

3.2 ノードの再接続を考慮した隣接ノード選択法

本研究の提案手法における隣接ノードを再選択する手順は，次のようになる．

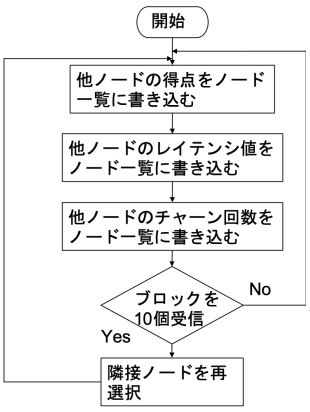

図 1 提案手法のフローチャート

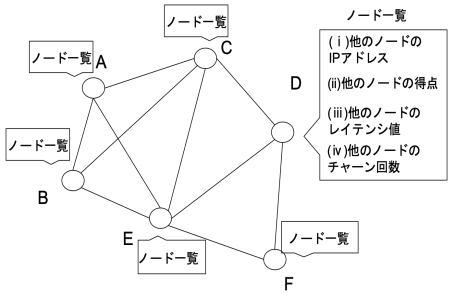

図 2 提案手法を適用したブロックチェーンネットワークの概要図

1. 各ノードは，ノード情報を保持している．ノード情報には，(ⅰ) ノードの IP アドレスまたはノード名，(ii) 他ノードの得点，(iii) レイテンシ，(iv) チャーン回数の 4 つの情報を記録する．
2. ノードは，他のノードからのブロックを送信する速度に応じた得点を，ノード情報に書き込む．
3. ノードは，他のノードのレイテンシ値を ping 通信によって測定し，ノード情報に書き込む．
4. ノードは，他のノードのチャーン回数を ping 通信によって測定し，ノード情報に書き込む．
5. 各ノードは，N 個のブロックを受信するたびに隣接ノードを更新する．ノード情報にあるノードを，(ii)，(iii)，(iv) の値を昇順にソートすることで，隣接ノードを再選択する．本研究の提案手法のフローチャートを，図 1 に示す．

提案手法におけるノード情報は，各ノードが保持している参加ノードのリストを基に実装する．ブロックチェーンにおける各ノードは，ネットワーク全体で大まかに共有されている参加ノードのリストから宛先ノードを選択する．例えば，Bitcoin であれば各ノードは他のノードの IP アドレスやノード名を保持している．ノードには直近でうまく接続できた隣接ノードが記憶されているので，ネットワークに再接続したときに素早く接続できる．図**??**は，提案手法を適用したブロックチェーンネットワークを局所的に示した概要図である．

3.3 評価指標

他のノードの得点は，青木らの研究における評価方法を基に得点づけする．青木らの提案手法では，あるノードからみた他のノードにそれぞれ得点をつけている．各ノードの得点をつけるための計算式は，次のようになる．

$$SCORE_x \Leftarrow T_{Message} - T_{Block} \tag{1}$$

$$SCORE_x \Leftarrow (1-P)\times SCORE_x + P\times(T_{Message} - T_{Block}) \tag{2}$$

$SCORE_x$ は，ノード x からメッセージを受信した時の得点である．ブロックの作成時刻は T_{Block}，メッセージの到着時刻は $T_{Message}$ で表される．メッセージの到着時刻からブロックを生成した時刻の差分を求めると，ブロックを生成されてからどの程度の時間でノード x からブロックを受信したかがわかる．よって，$SCORE_x$ の値が小さいノードほど，あるノードからみて通信効率の良いノードであることがわかる．Bitcoin においては，ブロックを送信する速度は inv メッセージを用いて計測し，inv メッセージが受信された時の得点である．

Bitcoin においては，メッセージの到着時刻を inv メッセージの到着時刻として，T_{INV} で表される．inv メッセージとは，ブロックを送信するノードが送信前に，送信先のノードが当該ブロックをすでに所持していないかを確認するためのメッセージである．inv メッセージを受信したノードがブロックを所持していない場合，getdata メッセージを返信してブロックの送信を要求する．ブロックを生成した時刻から inv メッセージを受信した時刻の差分で各ノードに得点をつけ，各ノードが N ブロックを受信するごとに，得点の低い順に隣接ノードを再選択する．Bitcoin では各ブロックはブロック生成時刻の情報を含み，各ノードは inv メッセージの受信時刻を取得可能なので，得点をつけるために他の情報を必要としない．

ここで，P は [0,1] の範囲内の重み付けパラメータである．青木らの研究によると P=1 のときに最も伝搬効率が良いので，本研究では青木らの研究に倣って P の値を 1 とする．ノード x からいずれかのブロックの inv メッセージを一度も受信していなければ，式 (3.1) を用いて得点が更新される．しかし，ノード x からいずれかのブロックの inv メッセージを一度でも受信しているならば，得点は式 (3.2) を用いて更新される．

レイテンシは，Bi らの研究を参考にして RTT 測定によって計測する．RTT 測定には ICMP ECHO を用いる．Bitcoin では，ノード間の ping 通信にかかった平均時間と最小時間について各ノードが保持している．あるノードが他のノードに ping を送信してから，ping が返却されるまでにかかった時間を計測して，レイテンシ値を決定する．このように，定期的に行われる ping 通信によって他のノードのレイテンシ値を更新していく．

他のノードのチャーン回数は，ノード間の ping 通信によって測定する．あるノードが他のノードに ping 送信を行い，それに応答した場合は，チャーンをしていないことがわかる．一方，あるノードが他のノードに ping 送信を行い，それに応答しなかった場合はチャーンを行なっていると考えることができる．あるノードが他のノードに ping を送信して応答がなかった場合，他のノードの IP アドレスのチャーン回数に 1 を加算する．このようにして，他のノードのチャーン回数を更新する．

他のノードのチャーン回数は，各 IP アドレスごとに計数する．Bitcoin では，各ノードは隣接ノードすべてのインデックス番号を保持している．他のノードのインデックス番号は，そのノードと接続した順に 0 から振り分けされる．インデックス番号をチャーン回数の計数に使うと，他のノードが再接続した場合はインデックス番号が更新されてしまう．よって，チャーン回数の計数には他のノードのインデックス番号ではなく，IP アドレスを用いる．

隣接ノードを再選択するタイミングは，青木らの研究を基にして実装する．青木らの研究では，ブロックチェーンネットワークに存在する各ノードそれぞれが，10 ブロックを受信するごとに隣接ノードの再選択を行なっている．本研究では青木らの提案手法に倣いつつ，N ブロック受信するごとに隣接ノードを再選択する．ブロックチェーンネットワークに存在する各ノードが N ブロックを受信するごとに，(ii)，(iii)，(iv) の値を昇順にソートする．

3.4 P2P ネットワークに初めて接続するノードの場合

P2P ネットワークに初めて接続するノードについては，本研究における隣接ノード選択法のシナリオが異なる．P2P ネットワークに初めて接続するノードは，ブロックやトランザクションのメッセージを送信することも，P2P ネットワークからの離脱も行なっていない．P2P ネットワークに初めて接続するノードに対応する IP アドレスに紐づけられたチャーン回数が 0 として計数されるのは適切でなく，メッセージ送信の速度やレイテンシ値についても測定していないので，再選択の指標にすることができない．

本研究の提案手法を適用したブロックチェーンネットワークに初めて接続するノードは，ネットワークにすでに接続している既存ノードの情報を用いて最適なノードとの接続を行う．P2P ネットワークに初めて接続するノードは，既存ノードからチャーン回数やブロック送信速度，レイテンシ値の情報を受け取り，それぞれの評価指標が良好であるノードに接続する．

4 考察

4.1 提案手法の有用性

本研究の提案手法では，青木らの提案手法 [4] と Bi らの提案手法 [3] を組み合わせることで，より高い精度で伝搬効率を向上できる．2 つの提案手法のうちいずれかのみを用いてブロックチェーンネットワークを構築した場合，次のような状況が想定される．例えば，コンピュータの OS がハングアップしているが，コンピュータはブロックチェーンノードとしてネットワークに接続しており ICMP ECHO を返信する状況が考えられる．このような状況では，Bi らの提案手法である物理ネットワークにおけるレイテンシ値を評価指標に隣接ノードを選択する方法よりも，ブロックチェーンネットワーク上のメッセー

ジ送信速度を評価指標とする青木らの提案手法を用いることで適切に隣接ノードを選択できる．あるいは，ブロックチェーンノードが正常に動作しないが，コンピュータの OS はハングアップせず ICMP ECHO を返信する状況も考えられる．このような状況では，青木らの提案手法ではなく Bi らの提案手法を用いることで適切に隣接ノードを選択できる．したがって，ブロックチェーンネットワークにおけるメッセージの計測が困難な状況では Bi らの提案手法，物理ネットワークにおけるメッセージの計測が困難な状況では青木らの提案手法を用いるといったように，2 つの提案手法を組み合わせることでいずれかのネットワークにおける障害を回避することができる．

4.2 ノード情報の制約条件

本研究の提案手法におけるノード情報は．各ノードがたかだか 1 桁の個数に制限する必要がある．各ノードが保持するノード情報の数を増やしていくと．最終的に各ノードがブロックチェーンネットワークにある全てのノードのノード情報を持つことになる．各ノードそれぞれがブロックチェーンネットワーク上のすべてのノードのノード情報を保持しているということは．中央集権的ではなく自律分散的であるブロックチェーンの設計思想に反することになる．

コストパフォーマンスの観点から考えても．ブロックチェーンネットワーク上に存在するノードそれぞれが全てのノードのノード情報を保持することは．ブロックチェーンのスケーラビリティ問題を解決することには繋がらない．したがって．各ノードが保有できるノード情報の数はたかだか 1 桁として制限することで．ブロックチェーンの設計思想に反することと，コストパフォーマンスの問題を回避する必要がある．

4.3 提案手法の適用範囲

本研究の提案手法は，Eclipse 攻撃に関して耐性がある．Eclipse 攻撃は，標的とするノードまたは標的とするノードのグループ全ての隣接ノードを悪意のあるノードに置き換えて，標的のノードをブロックチェーンネットワークから孤立させ，分断する攻撃である．本研究の提案手法では，隣接ノードを選択する際のランダム性を低くし，ブロックチェーンネットワークトポロジに規則性を与えているので，隣接ノードが悪意を持って操作される危険性が高まる．しかし本研究の提案手法においては，青木らの研究の提案手法を基にして，ブロックをより早く送信するノードが隣接ノードとして選択される．つまり，ノード間のブロックを生成するために必要なコンセンサスアルゴリズム計算の競争に勝利する計算力を持つノードが，優先的に隣接ノードとして選択される．したがって，攻撃者が悪意のある隣接ノードを自身のブロックチェーンノードの周囲に占領するためには，他のノードとのブロックを生成するための競争に勝たなければならないので，攻撃をするためのコストが増加する．よって，Eclipse 攻撃を根本的に解消することはできていないが，攻撃者は Eclipse 攻撃を実行するためには多大な労力を必要としているので，本研究の提案手法は耐性を備えている．

本研究の提案手法をシャーディング技術に適用した場合にも，伝搬効率が改善されることが期待できる．シャーディング技術においても，チャーン問題や下位レイヤとの不整合は起こりうる．したがって，トランザクションやブロックを効率よく伝搬できるノードを隣接ノードに再選択することで，P2P ネットワーク全体の伝搬効率が向上する．

5 おわりに

ブロックチェーンネットワークにおいて，接続先のノードがランダムに選択されることでいくつか問題が生じる．接続先のノードのチャーン率が高い場合や，物理ネットワークからみて不安定である場合には，通信が途切れやすいのでメッセージの伝搬が遅延する．伝搬遅延が起こると，メッセージ通信を効率よく行うことができなくなる．

ブロックチェーンネットワークでは，伝搬遅延が生じるとフォークが発生する．フォークが発生すると，各ノード間で異なるブロックを最新のブロックと見なすので，データの整合性が取れなくなる．また，フォークはセルフィッシュ・マイニング攻撃などの攻撃に弱く，セキュリティ上の大きなリスクとなる．

本研究の目的は，これらの課題を解決するために，ブロックチェーンネットワークにおける伝搬効率と安定性を向上させる枠組みを提案することである．伝搬効率を改善すると同時に，ブロックチェーンネットワークが安定して通信を行えるような手法を提案した．本研究では，チャーン問題による伝搬遅延に対する解決策を加えることで，より効率的で安全なブロックチェーンネットワークを構築できるような手法の実現を目指した．

今後の課題は，本研究の提案手法におけるセキュリティについて検討することや，本研究の提案手法が Bitcoin 以外のブロックチェーン基盤において適用できるかどうかを検討することである．

参考文献

[1] Mohamed Amine Ferrag, Makhlouf Derdour, Mithun Mukherjee, Abdelouahid Derhab, Leandros Maglaras and Helge Janicke, ”Blockchain Technologies for the Internet of Things: Research Issues and Challenges”, IEEE Internet of Things Journal, Volume: 6, Issue: 2 , April 2019.

[2] Muhammad Anas Imtiaz, David Starobinski, Ari Trachtenberg, Nabeel Younis, ”Churn in the Bitcoin Network: Characterization and Impact”, IEEE International Conference on Blockchain and Cryptocurrency (ICBC), 2019.

[3] Wei Bi, Huawei Yang, Maolin Zheng, “An Accelerated Method for Message Propagation in Blockchain Networks”, https://arxiv.org/abs/1809.00455, 2018.

[4] Yusuke Aoki and Kazuyuki Shudo, ”Proximity Neighbor Selection in Blockchain Networks”, IEEE Blockchain 2019, July 2019.