Bitcoin ネットワークにおける情報拡散妨害リスクの定量的評価

代表研究者　　笹　部　昌　弘　　奈良先端科学技術大学院大学 先端科学技術研究科 准教授

1 はじめに

ビットコインは Satoshi Nakamoto によって提唱された論文[1]に基づき開発された暗号通貨システムであり，国や銀行といった中央管理者の存在なしに，手数料を必須としない個人間での送金を実現している．ビットコインでは，取引情報の記録がブロックチェーンと呼ばれる分散型台帳としてシステムに参加する端末（ノード）間で共有される．端末間では Peer-to-Peer (P2P)ネットワーク（ビットコインネットワーク）が構築され，ある端末で新たに発生したトランザクションはビットコインネットワーク上にブロードキャストされる[2]．

ネットワーク上には複数のトランザクションをまとめてブロックを生成（マイニング）するマイナーと呼ばれる特別なノードが複数存在する．マイニングには高難度のハッシュ計算が伴うが，ブロックチェーンへの新たなブロックの追記に成功すると，システムから報酬が得られる仕組みが導入されており，マイナーは自身の計算資源（電力）の消費と引き換えに報酬の獲得を目指す．ここで，報酬の獲得とは，正確にはシステムから自身への送金を記したトランザクションを作成するブロック内に含め，そのブロックがブロックチェーンに追記されることで成立する．そのため，マイナーが報酬を獲得するためには，生成したブロックをビットコインネットワークを介して迅速に他のノードに拡散する必要がある．このように，マイナー間ではブロック生成とブロック拡散の 2 種類の競争が存在する．

ネットワーク上の各ノードは同じビットコイン・プロトコルに従い動作することが期待されるが，ソフトウェアはオープンソースで開発されており，改変が可能である．ブロック生成競争におけるハッシュ計算はそのランダム性の高さや計算結果の他のノードによる検証により改ざんが困難である一方，ネットワークを利用した攻撃の可能性が指摘されている[3]．[4]では，攻撃者が攻撃対象ノードとの間のすべての接続を独占し，ネットワークから隔離する Eclipse attack が提案されている．[5]では，単一の攻撃者がブロック転送時に設けられた正規のタイムアウト制御を悪用することで，特定のノードに対するブロックの伝搬を遅らせる攻撃（ブロック伝搬遅延攻撃）の可能性が指摘されている．特に，ブロック伝搬遅延攻撃は攻撃の実現が容易であるが,[5]では単一の攻撃者による 1 ホップのブロック伝搬における遅延攻撃のリスクのみが検討されている．

本研究では，特定のマイナーと結託した複数の攻撃者がブロック伝搬遅延攻撃を同時に行う，ブロック拡散妨害攻撃に着目する．シミュレーション評価により，攻撃者の数やネットワーク内の位置がブロック拡散妨害攻撃のリスクに与える影響を定量的に明らかにする．

2 ビットコインネットワーク上でのブロック拡散

2-1 ビットコインネットワーク

ビットコインネットワークは様々な種類とバージョンのビットコインクライアントが動作するノード間で論理的に構築される．本節では，ビットコインクライアントの代表例である，Bitcoin Core[6]におけるネットワーク構築のプロセスを紹介する．まず，新規ノードがビットコインネットワークに参加するためには，一つ以上の既存ノードの情報が必要となる．ビットコインネットワークに参加するノードは自身の IP アドレスによって識別される．新規ノードは，既存ノードの IP アドレスを管理する DNS サーバ（DNS シード）から接続先候補となるノードの情報を取得し，接続を試みる．ネットワークに接続した新規ノードは，以降，addr メッセージによりシステム内に存在するノードの情報を他のノードとやりとりすることができる．

各ノードでは，受信した addr メッセージの情報を基に，隣接ノードが IP アドレス空間上でできる限り偏らないよう，接続先候補の表を管理する．ビットコインネットワークは，本来，隣接ノード数（次数）に偏りの少ない，ランダムネットワークとなるよう設計されており，各ノードは，一定数（現状では 8）のノードを上限に，他のノードに接続要求を送る．一方，他のノードからの接続要求を受け入れることもできるが，外向き・内向き合わせた接続の合計数は最大 125 に制限されている．

公益財団法人電気通信普及財団
研究調査助成報告書　第35号　2020年度

ビットコインシステムでは，セキュリティの観点から，各ノードの接続関係を他のノードが直接把握することができないように設計されている[2]．Miller らは AddressProve と呼ばれる手法を用いることで，ネットワークトポロジの解析を行った[7]．その結果，大半のノードはデフォルトの出次数に近い 8–12 の次数を持つことが確認された一方，プロトコル仕様上の最大次数である 125 を大幅に上回るノードも複数存在することが示されている．また，こうした高次数ノードはマイニングプール（マイナーの集団）やウォレットサービスの運営者であることが指摘されている．4 章の評価では，[7]で観測されたノードの次数分布を基に，評価対象のビットコインネットワークを設計する．

また Bitnodes[8]では，クローラーと呼ばれるソフトウェアにより，ビットコインネットワーク上のすべての到達可能なノードを検出している．その結果，2019 年 6 月時点で，ビットコインネットワーク上には約 10000 台のノードが存在することがわかっている．また，Bitnodes では，ノードの地理的な分布情報や IP アドレス，クローラーからの遅延時間などを取得可能な API が提供されている．

2-2 ブロック拡散

ビットコインプロトコルに従い，隣接ノード間でブロックが伝搬される様子を図 1 に示す．図では，ノードX がノードYにブロックを転送する状況を表している．まず，ノードXは，自身がブロックを生成するもしくは受信すると，隣接ノードYに対して inv メッセージを送信することで，新たなブロックのメタ情報（ブロックハッシュ）を通知する．ブロックハッシュとは，SHA-256 のハッシュ関数によって得られる値であり，各ブロックにとってユニークな識別子となる．ノードYはノードXから受け取ったブロックハッシュを参照することで,対応するブロックを既に保持しているかどうかを判断する.ブロックを保持していない場合は，ノードYはノードXに対して getdata メッセージを送信して，ブロックの転送を要求する．ブロックサイズ（上限 1 MB）と比較すると，ブロックハッシュは 256 ビットとサイズが非常に小さく，ブロックハッシュによる事前確認を導入することで，ブロックの重複受信による通信帯域の浪費を防ぐことができる．転送要求を受け取ったノードXはブロックのデータを含む block メッセージを応答する．ブロックを受け取ったノードYはマイナーのハッシュ計算による結果や，ブロック内で確認されたすべてのトランザクションの正当性を検証し，問題がなければ自身のブロックチェーンに追加する．その後，自身の隣接ノードに対して同様の手順でブロックデータを転送する．

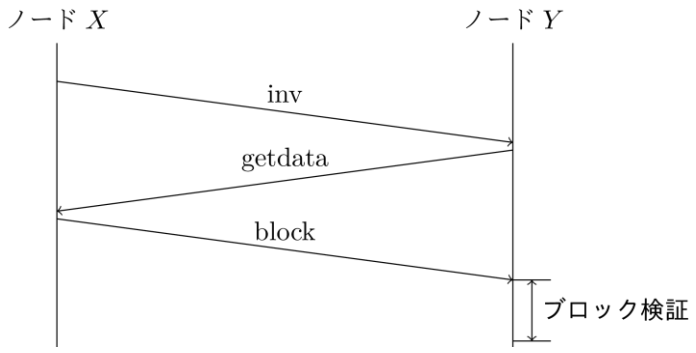

図 1 隣接ノード間でのブロック伝搬のプロセス

各隣接ノード間で上記のプロセスが繰り返し実行されることで，ブロックがビットコインネットワーク全体に拡散される．Decker らは実験用のノードをネットワークに参加する多数のノードに接続し，それらからの inv メッセージが到着した時刻を観測することで，ビットコインネットワークにおけるブロックの拡散時間の分析を行っている[9]．その結果，最初のブロックが受信されてからの経過時間は指数分布で近似でき，その中央値は約 6.5 秒，平均は 12.6 秒，また，40 秒経過時点では 5%のノードがブロックを受信していないことが示されている．ブロック拡散時間の増加はブロックチェーンの分岐（フォーク）につながる．ビットコインプロトコルでは，本来，全ノードが同一のブロックチェーンを保持することを期待しているが，フォークが生じた場合には最長のブロックチェーンを採用することが決められている．この機構を悪用することで，すでに使用されたコインを再び使用する 2 重支払い攻撃[10]等が可能となるため，迅速なブロック拡散は重要な課題である．

ブロック拡散遅延にともなう脆弱性に対する対策として，プロトコルの仕様の見直しも行われている．例えば，ビットコインクライアントの代表となる Bitcoin Core [6]のバージョン 0.10.0 以降では，ブロック

データではなくブロックヘッダ のハッシュ値を inv メッセージで通知し，getheaders メッセージでそれに対応するヘッダを要求するプロトコルが実装されている．ブロックデータと比較してブロックヘッダのサイズは 80 バイトと小さいため， ヘッダを迅速に転送し，各ノードが最長のヘッダーチェーンを保持することで，フォークの発生を早期に発見できる利点がある．さらに，inv メッセージの代わりに新規ブロックのヘッダを含む headers メッセージを送信するプロトコルが提案されており[11]，Bitcoin Core 0.12 で実装されている[12]．この実装により，ブロックヘッダの転送によるオーバーヘッドを緩和することができ，ブロック拡散の速度を高めるという利点がある．

3 ブロック拡散妨害攻撃

3-1 隣接ノード間でのブロック伝搬遅延攻撃

図 1 では，隣接ノード間におけるブロック伝搬の様子を示したが，あるノードは複数の隣接ノードから同一のブロックに対する inv メッセージを受信する可能性がある．ビットコインプロトコルでは，通信帯域の使用量を抑えるために，最初にブロックを通知してきたノードに対してのみ，ブロックデータを要求するように設計されている．ただし，ノードやネットワークの一時的な不調によりブロックの伝搬に時間がかかる場合を想定し，タイムアウト制御が設けられている．なお，ブロック伝播遅延攻撃[5]が指摘された時点ではタイムアウトは 20 分であったが[1]，その後 10 分へと変更されている[2]．タイムアウトが発生すると，inv メッセージを受信した他のノードにブロック転送を要求する．

[5]では，攻撃者がこのタイムアウト制御を悪用し，特定のノードへのブロックの転送を遅らせる，ブロック伝搬遅延攻撃のリスクを指摘している．隣接ノード間でのブロック伝搬遅延攻撃のプロセスを図 2 に示す．図では，攻撃者Aが攻撃対象ノードVに攻撃を仕掛ける様子を示している．まず，攻撃者Aはブロックを受信すると，通常のビットコインプロトコルと同様に，攻撃対象Vに対して inv メッセージを送信する．この時，攻撃成功のためには，攻撃者Aが攻撃対象Vにとって inv メッセージの最初の送信者となる必要がある．[5]では，攻撃者がブロック受信後の検証プロセスを省略することで，この条件が満たされる可能性を向上させているが，本研究では，さらに，攻撃者Aが自身のブロック受信プロセスと並行して inv メッセージを攻撃対象Vに送信することで，攻撃成功の可能性を向上させる方式を想定する．攻撃者Aは攻撃対象Vからのブロックデータの要求(getdata)に対してblock メッセージではなく，自身の生存を示すpong メッセージを返す．その結果，タイムアウト発生まで，攻撃者Aは攻撃対象Vのブロック受信を妨害できる．

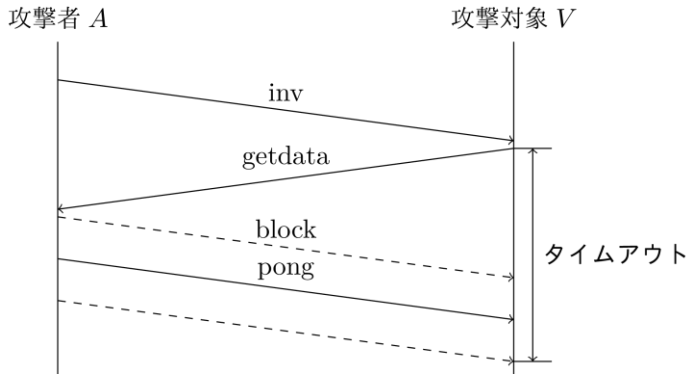

図 2 隣接ノード間でのブロック伝搬遅延攻撃のプロセス

3-2 攻撃ノードの配置戦略

ブロック拡散妨害攻撃の効果は，ネットワーク上での攻撃者の台数と位置により変化すると考えられる．本節では，攻撃者の立場から，攻撃の効果を最大限に発揮するための攻撃者の配置戦略を検討する．

ビットコインネットワークをグラフ$G=(\mathcal{V},\mathcal{E})$で表現する．ここで，$\mathcal{V}=\{v_i : i=1,2,\ldots,N\}$はノードの集

[1] https://github.com/bitcoin/bitcoin/pull/5608

[2] https://github.com/bitcoin/bitcoin/pull/7832

合， $\mathcal{E}$はリンクの集合とする．まず，一つ目の配置戦略として，多くの隣接ノードを持つノード（高次数ノード）が攻撃者となることで，ブロック伝搬遅延攻撃の被害者となるノードの増加が期待される．これは，

$$C_{\mathrm{D}}(i) = \frac{k_i}{N-1} \tag{1}$$

で表されるノードv_iの次数中心性$C_{\mathrm{D}}(i)$ [13]の降順に攻撃者を配置する戦略であり，以降では次数中心性配置戦略と呼ぶ．ここで，k_iはノードv_iの次数を表す．

一方，ブロック伝搬遅延攻撃の実行には攻撃者自身が攻撃対象のブロックに対する inv メッセージを受信する必要がある（図 2）．攻撃者が inv メッセージを迅速に受信するための戦略としては，例えば，攻撃者の媒介中心性[13]を高めることが考えられる．ノードv_iの媒介中心性$C_{\mathrm{B}}(i)$とは，任意の 2 ノード間の最短経路上にv_iが存在する割合であり，次式で与えられる．

$$C_{\mathrm{B}}(i) = \frac{2}{(N-1)(N-2)} \sum_{j \in \mathcal{V}, j \neq i} \sum_{k \in \mathcal{V}, k \neq i, k < j} \frac{n_{jk}(i)}{n_{jk}} \tag{2}$$

ただし，n_{jk}はノードv_j, v_k間を結ぶ最短経路の数，$n_{jk}(i)$はその中でノードv_iを含む最短経路の数をそれぞれ表す．媒介中心性の降順に攻撃者を配置する戦略を以降では媒介中心性配置戦略と呼ぶ．

4 シミュレーション評価

4-1 シミュレーション設定

評価用のビットコインネットワークとしては,[7]で観測された実際のビットコインネットワークにおける次数分布と既存の Bitcoin-Simulator[14]の設定を参考に以下のように作成した．ノードの総数は 6000 台とし，そのうち 16 台をマイナーとする．各ノードの地理的な位置は，Bitnodes[8]におけるノードの地理的分布に関する統計情報を基に決定する．隣接ノード間の伝搬遅延，帯域情報は，両者の地理情報と Bitcoin-Simulator の設定を基に決定する．また，2.1 節で述べたように，マイナーは高次数ノードとなる傾向があるため，次数の範囲を 700–800 とした一様分布に，通常ノードは[7]の次数分布にそれぞれ従うよう，各ノードの次数を決定した．

ブロック拡散妨害攻撃の基本特性を明らかにするために,離散事象型シミュレータを Java 言語で作成した．攻撃者となるノードは，ノードの中から$\alpha = \{0, 1, 5, 10, 15\}$%の割合で選択する．なお，攻撃者の配置方法としては，3.2 節で述べた次数中心性配置戦略と媒介中心性配置戦略に加えて，ランダムに配置する戦略（ランダム配置戦略）を用いる．また，中心性の計算には NetworkX[15]を利用する．すべてのノードが同一のブロックチェーンを保持しているという状況を初期状態とし，シミュレーション開始時$(t = 0)$に 16 台のマイナーの中からランダムに選ばれた 1 台のマイナーがブロックの生成に成功する．攻撃者はこのマイナーの協力者とし，以降，ビットコインプロトコル及びブロック拡散妨害攻撃に従い，ビットコインネットワーク上でのブロックの拡散と妨害が行われる．ここで，ブロックのサイズは上限が 1 [MB]となっているが，[14]の執筆当時の 10000 ブロックの平均サイズを考慮し，0.534 [MB]と設定した[16]．また，ブロックの検証時間を 0.1 秒，タイムアウト時間を 600 秒とする．表 1 に各種パラメタの値を示す．以降では，独立した 1600 回の試行の平均を示す．

表 1 評価シナリオ

パラメタ	値
ノード数 N	6000
マイナー数 M	16
攻撃者の割合 α	0，1，5，10，15［%］
ブロックサイズ B_s［MB］	0.534
ブロック検証時間 T_v［s］	0.1
タイムアウト時間 T_o［s］	600

4-2 攻撃者の台数による影響

まず，攻撃者の台数がブロック拡散妨害攻撃に与える影響を評価する．攻撃者の配置戦略としてランダム配置戦略を用いた場合における，攻撃者の割合を変化させた場合のブロック取得ノードの割合の推移を図 3 に示す．ただし，ブロック取得ノードの割合は，攻撃者を除く全ノードの中でブロックを取得したノードの割合とする．また，ビットコインプロトコルにおけるブロック生成の平均時間間隔が 600 秒であることを考慮し，図 3 では$t = [0, 600]$の範囲に着目している．

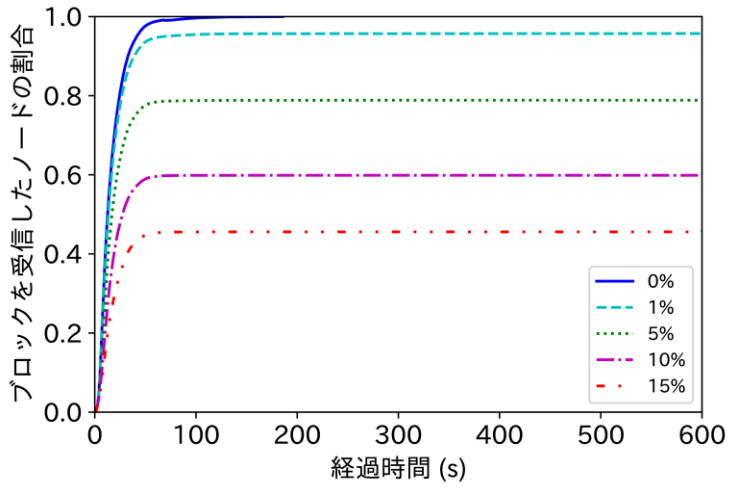

図 3 攻撃者の割合αとブロックを取得したノードの割合との関係（攻撃者の配置：ランダム，$t = [0, 600]$）

図より，攻撃者が存在しない場合($\alpha = 0$)，速やかにブロックの拡散が行われ，$t = 186$の時点ですべてのノードがブロックを取得できていることがわかる．一方，攻撃者が存在する場合は，攻撃を受けたノードはタイムアウト時間である 600 秒が経過するまでブロックの取得が中断される．その結果，攻撃者の割合αの増加に従い，600 秒までに一定の割合のノードがブロックを取得できていないことが確認できる．特に，攻撃者の割合αに対して 600 秒までにブロックを取得できないノードの割合が大きいことがわかる．このような状況で次のブロックが生成・拡散されるとブロックチェーンのフォークが生じることとなり，攻撃者と結託したマイナーが自身のブロック拡散を優位に進められる可能性を示唆している．

通常であれば，ブロック生成の平均時間間隔が 600 秒であることから，同一のブロックに対する 2 回以上の攻撃を受信する可能性は低いが，ブロック拡散妨害攻撃の基本特性を明らかにするために，攻撃者の割合がブロック取得ノードの割合の推移に与える影響を$t = [0, 1800]$の範囲で示す（図 4）．図より，タイムアウト時間 600 秒ごとに攻撃から復帰したノードがブロックを取得あるいは攻撃を受信することで，ブロック取得ノードの割合が階段状に増加する様子が確認できる．

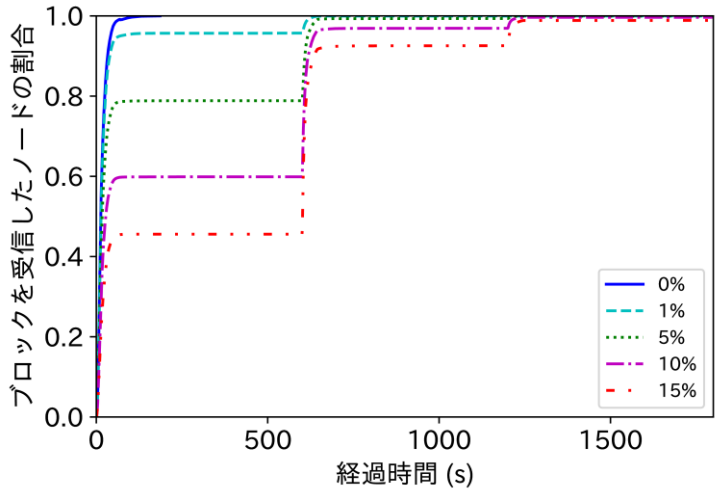

図 4 攻撃者の割合αとブロックを取得したノードの割合との関係（攻撃者の配置：ランダム，$t = [0, 1800]$）

4-3 攻撃者の配置戦略による影響

次に，3.2 節で述べた攻撃者の配置戦略がブロック拡散妨害攻撃に与える影響を評価する．図 5 は，$\alpha = 1$ とした場合の各配置戦略におけるブロック取得ノードの割合の推移を示している．図より，ランダム配置戦略と比較して，次数中心性配置戦略と媒介中心性配置戦略は同じ攻撃者の割合でもより攻撃のリスクが高まることが確認できる．

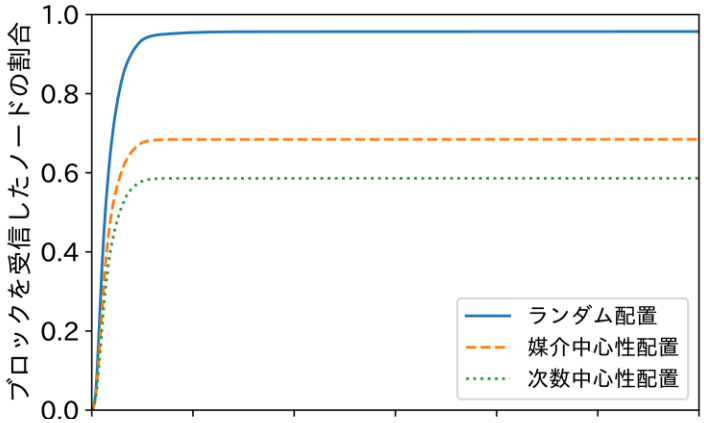

図 5 攻撃者の配置戦略とブロックを取得したノードの割合との関係

3.2 節で述べたように，次数中心性配置戦略では，攻撃者が多くの隣接ノードを獲得することで攻撃対象者を増やす効果が，媒介中心性配置戦略では，攻撃者がブロックの伝播経路上に位置しやすくする，すなわち攻撃機会を獲得しやすくする効果が期待されるが，図より，次数中心性配置戦略の方が攻撃のリスクが高いことがわかる．次数中心性配置戦略は攻撃者が隣接ノードを増やすことで実現できることから，媒介中心性配置戦略と比較すると実現の容易性が高く，また，$\alpha = 1$という少数の攻撃者でも半数近くのノードへのブロック伝搬を妨害できていることから，ブロック拡散妨害攻撃のリスクは高いことがわかる．

5 関連研究

本章では，ビットコインプロトコルを悪用した攻撃に関する関連研究を紹介する．ビットコインプロトコ

ルを悪用した攻撃は，複数のマイナーが結託し，高い計算能力を獲得することで実現可能な攻撃（計算能力型攻撃[1, 17]）とビットコインネットワークの脆弱性を利用した攻撃（ネットワーク型攻撃[4, 5, 18]）の2種類に大別できる．以降ではそれぞれの攻撃の紹介とそれらの連携リスクについて述べる．

[1]では悪意のある攻撃者がネットワーク全体の計算能力の過半数以上を支配する 51%攻撃のリスクが提示されている．51%攻撃により，攻撃者はマイニングを寡占化することで，すでに使用されたコインを再利用する2重支払い攻撃[10]などの悪用が可能となる．[17]では，51%攻撃で想定されていた過半数の計算能力よりも低い，33%以上の計算能力を攻撃者が保持するだけでもブロックチェーンの書き換えが可能となる，利己的マイニング(selfish mining)のリスクが指摘されている．利己的マイニングでは，攻撃者がマイニングに成功したブロックをすぐにブロードキャストせずに，公開されているブランチ（公開ブランチ）から派生した非公開のブランチ（秘匿ブランチ）を作成する．秘匿ブランチの優位性（公開ブランチからの差分ブロック数）が十分大きい場合は，秘匿ブランチへのブロック追記を継続する．一方，他のマイナーによる公開ブランチへのブロック追記により秘匿ブランチの優位性がほとんどなくなった場合，攻撃者は秘匿ブランチを公開する．ここで，秘匿ブランチが公開ブランチよりも長くなることから，秘匿ブランチが新たな公開ブランチとしてネットワーク内での合意を得ることができる．その結果，攻撃者はシステムから報酬を得られるとともに，正規のマイナーによる過去のブロック生成が無効化され，このことはシステム全体としてのブロック生成レートの低下，そしてハッシュ計算の難易度の低下へとつながる．

こうした計算能力型攻撃の実現には，システム内での一定量の計算能力が求められるため，システム規模の増加に対して攻撃のリスクは低下する傾向がある．しかしながら，ネットワーク型攻撃により計算能力型攻撃の実現可能性が高まるリスクが指摘されている[4, 5, 18, 19]．[4]では，攻撃者が攻撃対象ノードとの接続を独占する事で，ネットワークから隔離する Eclipse attack が提案されている．Eclipse attack では，攻撃対象ノードが保持する管理表（2.1 節を参照）に含まれる IP アドレスを自身の管理下にある IP アドレスで埋め尽くすことで，攻撃対象ノードを孤立させ，正当なブロックチェーンを把握できないようにする．その結果，51%攻撃，2 重支払い攻撃，利己的マイニングといった前述の攻撃と併用することで攻撃の実現可能性を向上できる．実際に，[19]では，Eclipse attack と利己的マイニングを連携させた攻撃が提案されている．

[18]では Border Gateway Protocol (BGP) [20]ハイジャック攻撃が提案されている．ビットコインネットワークはインターネット上に構築された論理的なネットワークである．そのため，ビットコインネットワーク上でのノード間の情報のやり取りは下位のインターネット上でのルーチングに影響を受ける．インターネットは多数の Autonomous System (AS)で構成されており，AS 間のルーチングは BGP により実現されている．BGP ハイジャック攻撃では，不正な経路情報を広告する AS を配置することで，インターネット上での BGP ルーチングを妨害し，その結果，ビットコインネットワーク上での情報伝播を阻害する．特に，ビットコインネットワーク上のノードが所属する AS には偏りがあることがわかっており（全体の 30%が 13 の AS に，50%が 50 の AS に所属する），それら少数の AS を経由するルーチングを妨害することで攻撃を成功させることができる．

[5]では，単一の攻撃者がブロック転送時に設けられた正規のタイムアウト制御を悪用することで，特定のノードに対するブロックの伝搬を遅らせる攻撃（ブロック伝搬遅延攻撃）の可能性が指摘されている．この攻撃は，攻撃者が攻撃対象ノードに対して少なくとも一つの接続を確立することで実現できるという点で，Eclipse attack や BGP ハイジャックと比較して攻撃の実現可能性が高い．[5]では単一の攻撃者によるブロック伝搬遅延攻撃のリスクのみに着目していた．本研究では，この攻撃を特定のマイナーと複数の攻撃者が結託して行うことで，競争相手となるマイナーからのネットワークへのブロック拡散を遅らせ，相対的に自身のブロック拡散を優位に進める，ブロック拡散妨害攻撃の可能性を検討した．

6 まとめ

本研究では，あるマイナーが複数の攻撃者と結託し，ビットコインネットワーク上での競合マイナーのブロック伝搬を妨害する，ブロック拡散妨害攻撃に着目した．実際のビットコインネットワークの特徴を考慮したシミュレーションにより，攻撃者の数やネットワーク内での位置がブロック拡散妨害攻撃のリスクに与える影響を評価した．その結果，攻撃者数の増加割合に対して，平均ブロック生成間隔である 600 秒までにブロックを取得できないノードの増加割合が大きくなることが確認された．また，攻撃者の配置に関しては，

次数中心性配置戦略がランダム配置戦略や媒介中心性配置戦略よりも攻撃のリスクを高めることを明らかにした．今後の課題としては，このようなブロック拡散妨害攻撃への対策法の検討とその効果の評価が挙げられる．

【参考文献】

[1] S. Nakamoto, “Bitcoin: A Peer-to-Peer Electronic Cash System,” available at https://bitcoin.org/bitcoin.pdf, 2008.

[2] F. Tschorsch and B. Scheuermann, “Bitcoin and Beyond: A Technical Survey on Decentralized Digital Currencies,” IEEE Security and Privacy, vol.18, no.3, pp.2084–2123, 2016.

[3] T. Neudecker and H. Hartenstein, “Network Layer Aspects of Permissionless Blockchains,” IEEE Communications Surveys and Tutorials, vol.21, no.1, pp.838–857, 2019.

[4] E. Heilman, A. Kendler, A. Zohar, and S. Goldberg, “Eclipse Attacks on Bitcoin’s Peer-to-Peer Network,” Proc. of 24th USENIX Security Symposium, pp.129–144, 2015.

[5] A. Gervais, H. Ritzdorf, G.O. Karame, and S. Capkun, “Tampering with the Delivery of Blocks and Transactions i n Bitcoin,” Proc. of the 22nd ACM SIGSAC Conference on Computer and Communications Security, pp.692–705, 2015.

[6] “BitcoinCore,” available at https://bitcoincore.org/.

[7] A. Miller, J. Litton, A. Pachulski, N. Gupta, D. Levin, N. Spring, and B. Bhattacharjee, “Discovering Bitcoin’s Public Topology and Influential Nodes,” available at http://cs.umd.edu/projects/coinscope/coinscope.pdf, 2015.

[8] “Bitnodes,” available at https://bitnodes.earn.com.

[9] C. Decker and R. Wattenhofer, “Information Propagation in the Bitcoin Network,” Proc. of IEEE P2P 2013, pp.1–10, 2013.

[10] G.O. Karame, E. Androulaki, and S. Capkun, “Double-spending Fast Payments in Bitcoin,” Proc. of the 2012 ACM Conference on Computer and Communications Security, pp.906–917, 2012.

[11] “BIP130,” available at https://github.com/bitcoin/bips/blob/master/bip-0130.mediawiki.

[12] “Bitcoin Core version 0.12.0 released,” available at https://bitcoin.org/en/release/v0.12.0#how-to-upgrade.

[13] V. Latora and M. Marchiori, “A Measure of Centrality Based on Network Efficiency,” New Journal of Physics, vol.9, no.6, pp.188–188, 2007.

[14] A. Gervais, G.O. Karame, K. Wüst, V. Glykantzis, H. Ritzdorf, and S. Capkun, “On the Security and Performance of Proof of Work Blockchains,” Proc. of the 2016 ACM SIGSAC Conference on Computer and Communications Security, pp.3–16, 2016.

[15] “NetworkX,” available at https://networkx.github.io/documentation/stable/index.html.

[16] “Blockchain.info,” available at https://www.blockchain.com/ja/pools.

[17] I. Eyal and E.G. Sirer, “Majority Is Not Enough: Bitcoin Mining Is Vulnerable,” Proc. of Financial Cryptography and Data Security, pp.436–454, 2014.

[18] M. Apostolaki, A. Zohar, and L. Vanbever, “Hijacking Bitcoin: Routing Attacks on Cryptocurrencies,” Proc. of 2017 IEEE Symposium on Security and Privacy (SP), pp.375–392, 2017.

[19] K. Nayak, S. Kumar, A. Miller, and E. Shi, “Stubborn Mining: Generalizing Selfish Mining and Combining with an Eclipse Attack,” Proc. of 2016 IEEE European Symposium on Security and Privacy (EuroS & P), pp.305–320, 2016.

[20] “RFC 4271 - A Border Gateway Protocol 4 (BGP-4),” available at https://tools.ietf.org/html/rfc4271.

〈発　表　資　料〉

題　　名	掲載誌・学会名等	発表年月
Bitcoin ネットワーク上でのブロック拡散遅延攻撃における攻撃者数の影響	電子情報通信学会ソサイエティ大会講演論文集 B-11-10:166	2019 月 9 月
ビットコインネットワークにおけるブロック拡散妨害攻撃のリスク評価	電子情報通信学会・技術研究報告 119 (298):1-6	2019 年 11 月