様　式　Ｃ－１９、Ｆ－１９－１、Ｚ－１９　（共通）

科学研究費助成事業　　研究成果報告書

令和　４ 年　 ４ 月 ２７ 日現在

機関番号：１４６０３
研究種目：基盤研究(C)（特設分野研究）
研究期間：2019～2021
課題番号：１９ＫＴ００４５

研究課題名（和文）Bitcoin型競争的情報拡散に基づく合意形成における情報拡散妨害のリスク分析

研究課題名（英文）Analysis of Interruption Risk of Information Diffusion in Consensus Formation based on Bitcoin-like Competitive Information Diffusion

研究代表者
笹部　昌弘（Sasabe, Masahiro）

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

研究者番号：１０３７９１０９

交付決定額（研究期間全体）：（直接経費）　　3,300,000円

研究成果の概要（和文）：暗号通貨システムBitcoinは，ブロックチェーン技術により，悪意のあるユーザを含む不特定多数のユーザ間における取引台帳に対する合意を自律分散的に形成する．本研究では，ブロックチェーンの耐改ざん性に寄与する，競争的情報拡散の仕組みにおいて，正規の情報拡散を妨害できるリスクに着目する．特に，感染症伝播モデルに基づく新たな数理モデルとなるstandby-interrupted-retrieved-attackable (SIRA)モデルを確立し，攻撃者数，ネットワークの形状など種々の要素が妨害リスクに与える定量的に明らかにした．さらに，拡散妨害リスクを軽減するための対策手法を確立した．

研究成果の学術的意義や社会的意義
社会的意義としては，Bitcoinシステムにおける競争的情報拡散メカニズムに対する妨害リスクを，攻撃者数，攻撃速度，妨害からの復帰速度，ネットワークの形状，攻撃者の位置など，様々な観点から定量的に分析するとともに，その対策手法を提案し，有効性を示している点が挙げられる．
なお，競争的情報拡散の仕組みはBitcoinシステムに限らず，SNS上でのマーケティングや世論形成など，他のシステムにも遍在する仕組みとなるため，提案したSIRAモデルの活用が期待できる．

研究成果の概要（英文）：With the help of blockchain technology, the cryptocurrency system Bitcoin achieves consensus on the ledger among anonymous users in a distributed manner. We focus on the interruption risk of the competitive information diffusion mechanism, which plays one of the key roles in achieving the tamper-proof nature of blockchain. In particular, with the help of the deterministic nonlinear model for the propagation of infectious diseases in mathematical epidemiology, we have developed standby-interrupted-retrieved-attackable (SIRA) models. Through numerical evaluation, we have quantitatively revealed the interruption risk and further proposed countermeasures against it.

研究分野：情報ネットワーク

キーワード：競争的情報拡散　Bitcoin　情報拡散妨害　リスク分析　感染症伝播モデル　対策手法

１．研究開始当初の背景

暗号通貨システム Bitcoin の登場は，社会に大きな影響を与えただけでなく，学術的にも，悪意のあるユーザを含む不特定多数のユーザ間での高信頼かつ自律分散的な合意形成の実現という点で重要である．Bitcoin プロトコルにおける合意の対象は取引台帳であり，これを取引情報の塊であるブロックの列（ブロックチェーン）として実現している．新たなブロックの生成には過去のブロック情報と高難度なパズル的計算が必要であり，また，ブロックチェーンの追記に成功したユーザはシステムと取引利用者から報酬を得られる．その結果，ネットワークを介したユーザ間での情報拡散競争とブロック生成競争が発生し，これがブロックチェーンの耐改ざん性を実現している．

一方で，ブロック生成競争や情報拡散競争に対する攻撃の可能性も指摘されている．ブロック生成競争に関しては，その本質はユーザ間の処理能力競争であるため，複数ユーザ間での結託による処理能力の増大，特定のユーザへの攻撃による処理能力の低下などが主な攻撃手法となる．一方，ブロック拡散競争への攻撃手法に関しては，攻撃対象となるユーザを孤立させる Eclipse 攻撃や攻撃対象となるユーザの生成したブロックの伝播を阻害するブロック伝播妨害などが挙げられる．これらの中で，最も低コストで実現可能な攻撃はブロック伝播妨害となるが，[1] では，ユーザ間での１ホップのブロック伝播に対する攻撃の可能性についてのみ検討しており，Bitcoin ネットワーク全体としてのブロック拡散妨害のリスクに関しては未知である．ブロックの正常な拡散はブロックチェーン技術の根幹を担うため，攻撃者の台数やネットワーク内での位置，さらにはネットワークの形状がブロック拡散妨害の効率にどのような影響を与えるのかを解明することは急務である．

２．研究の目的

図 1 左は，Bitcoin ユーザ（ノード）間で構築される Peer-to-Peer (P2P) ネットワーク上にブロック生成を試みる特別なユーザであるマイナー m, o が存在し（五角形），マイナー o 側がマイナー m のブロック拡散を妨害する様子を示している．まず，マイナー m が先にブロック生成に成功したとする．マイナー m が報酬を得るためには，他のブロックよりも先にこのブロックを他のユーザによりブロックチェーンに追記してもらう必要があるため，まず隣接ノードにブロックを転送する（図１左）．その後も隣接ノード間でブロックが転送されるが，マイナー o 側の攻撃者となる２台のノード（菱形）は自身から下流のノードへのブロック伝播を妨害する．その結果，後続のマイナー o がブロック拡散競争で逆転できる可能性が生じる．

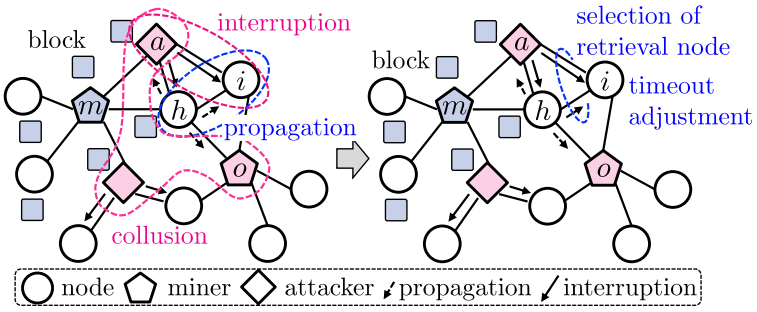
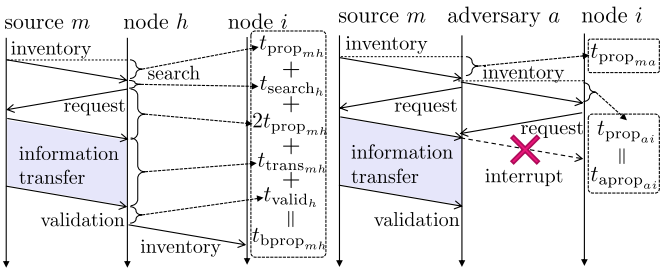


図 1: ブロックの拡散・妨害の様子（左）と対策手法（右）

ここで隣接ノード間のブロック伝播は図 2a に示すプル型で実現される．例えば，図１左において，ノード h は取得したブロックの正当性を検証後，隣接ノード i にブロックの情報を伝える．ノード i は当該ブロックを保持していない場合，ノード h にブロックを要求することになるが，ここで，ノード i と隣接する攻撃者 a が，図 2b に示すように，ブロックの検証を省いてノード h よりも先にブロック情報をノード i に通知し，実際にはブロックを転送しない場合，Bitcoin プロトコルにおけるタイムアウト時間 t_{TO} だけノード i のブロック取得を妨害できる．



(a) 正常なブロック伝播　　(b) ブロック伝播妨害

図 2: 隣接ノード間でのブロックの伝播・妨害の様子

[1] では，このようなブロック伝播の妨害に関して，攻撃者と攻撃対象者のペア間での攻撃成功確率に着目していた．本研究では，攻撃者が Bitocin ネットワーク内の複数箇所に侵入しブロック伝播攻撃を面的に行う，ブロック拡散妨害に着目する．このブロック拡散妨害は，Bitcoin ネットワークの形状，攻撃者の台数やネットワーク上での位置などにより，その効果が大きく影響を受けると考えられる．本研究では，感染症の伝播に着想を得た，妨害あり情報伝播モデルを確立するとともに，その複雑ネットワーク上での挙動を解析することで，ブロック拡散妨

害のリスクを解明することを目的としている．

３．研究の方法

研究の方法としては，まず，ブロック拡散妨害攻撃を感染症の伝播モデルに着想を得た，数理疫学的アプローチによりモデル化し，そのリスクを定量的に明らかにする．なお以降では，説明の簡単のため Bitcoin システムを前提としているが，提案するモデル自体は，より一般的な競争的情報拡散システムへの適用が可能である．次に，実際の Bitcoin ネットワークを考慮した詳細なシミュレーション評価により，拡散妨害リスクを定量的に評価するとともに，その対策手法について検討する．以降，それぞれについて説明する．

(1) 完全グラフ上でのブロック拡散妨害攻撃のモデル化 (Scalar SIRA モデル)

Bitcoin ネットワーク上でのブロックの伝播は感染症の伝播に類似しており，上記のブロック伝播に近い感染モデルとして Susceptible-Infected-Recovered (SIR) モデル [2] がある．本研究では SIR モデルに着想を得た上で，妨害ありのブロック伝播を新たに SIRA (Standby-Interrupted-Retrieved-Attackable) モデルとして確立する（図 3）．システム内の攻撃者の割合を α $(0 \leq \alpha \leq 1)$ とする．SIRA モデルでは，ユーザは，ブロックを保持しないスタンバイ状態 S_0 から始まり，ブロックを受信するとブロック保持状態 R に，攻撃を受信すると被攻撃状態 I へと遷移する．状態 I からはタイムアウト発生後，復旧状態 S_1 へと遷移し，以降，ブロックか攻撃を受信するとそれぞれ状態 R, I へと遷移する．一方，攻撃者は，ブロック未保持状態 S_0 から始まり，ブロックか攻撃を受信すると攻撃可能状態 A に遷移する．

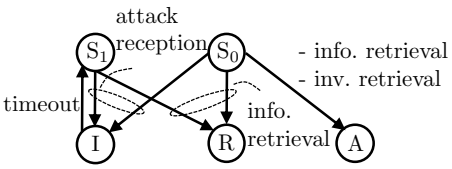


図 3: SIRA モデル

なお，システムが $N > 0$ 台のノードで構成され，各ノードが他のノードと単位時間あたり率 $c > 0$ でランダムに通信可能であると仮定すると，平均場近似の考えにより，状態 S_0, S_1, I, R, A をとるノード数 S_0, S_1, I, R, A の時間変化は以下の連立微分方程式でモデル化できる．

$$\dot{S}_0 = -S_0 c(\beta_0 R + \beta_1 A), \qquad \dot{S}_1 = -S_1 c(\beta_0 R + \beta_1 A) + \delta I,$$
$$\dot{I} = ((1-\alpha)S_0 + S_1)\beta_1 cA - \delta I, \qquad \dot{R} = ((1-\alpha)S_0 + S_1)\beta_0 cR,$$
$$\dot{A} = \alpha S_0 c(\beta_0 R + \beta_1 A).$$

例えば，$\mathrm{S}_0 \to \mathrm{R}$ の遷移は，状態 S_0 のノードがユーザであり（率 $(1-\alpha)S_0$），かつ状態 R のユーザからブロックを受信する（率 cR）と生じる．その他の遷移も同様に捉えることができる．ここで，$\delta = t_{\mathrm{TO}}^{-1}$ であり，β_0, β_1 に関しては，図 2 の処理フローにおいて，$\beta_{0_{ij}} = t_{\mathrm{bprop}_{ij}}^{-1}, \beta_{1_{ij}} = t_{\mathrm{aprop}_{ij}}^{-1}$ と定義した上で，各ノード i, j 間 $(i, j \in \mathcal{N}, i \neq j)$ に対して，$\beta_{k_{ij}} = \beta_k$ $(k \in \{0, 1\})$ を仮定する．なお原理上，妨害速度の方が拡散速度よりも速い，すなわち，$\beta_1 > \beta_0 > 0$ が成立する．

このような系において，$\alpha, \beta_0, \beta_1, \delta$ がブロック拡散速度に与える影響を数理的に解析する．後述のネットワーク上での SIRA モデルと区別するために，上記のモデルを Scalar SIRA モデルと呼ぶ．

(2) 一般的なネットワーク上でのブロック拡散妨害攻撃のモデル化 (Network SIRA モデル)

実際の Bitcoin ネットワークは次数（隣接ノード数）分布に偏りのある構造を持つことが観測されている．この場合，前述の平均場近似の前提とは異なり，あるノードの状態遷移に影響を与えるのはその隣接ノードの集合に限られる．近年，スケールフリーネットワークなど複雑ネットワーク上での感染症伝播モデルに関する研究が進められている [2]．これらの知見を基に，前述の Scalar SIRA モデルをネットワーク上のモデルとなる，Network SIRA モデルに拡張する．

具体的には，ネットワーク上に存在する N 台のノード $\mathcal{N} = \{1, \ldots, N\}$ に対して，各ノード $i \in \mathcal{N}$ が状態 S_0, S_1, I, R, A である確率を，それぞれ $S_{0_i}, S_{1_i}, I_i, R_i, A_i$ と定義すると，それらの時間推移は以下の連立微分方程式でモデル化できる．

$$\dot{S}_{0_i} = -S_{0_i}(\sum_{j\in\mathcal{V}} \beta_{0_{ji}} R_j + \sum_{j\in\mathcal{V}} \beta_{1_{ji}} A_j), \qquad \dot{S}_{1_i} = -S_{1_i}(\sum_{j\in\mathcal{V}} \beta_{0_{ji}} R_j + \sum_{j\in\mathcal{V}} \beta_{1_{ji}} A_j) + \delta I_i,$$
$$\dot{I}_i = ((1-\alpha_i)S_{0_i} + S_{1_i}) \sum_{j\in\mathcal{V}} \beta_{1_{ji}} A_j - \delta I_i, \qquad \dot{R}_i = ((1-\alpha_i)S_{0_i} + S_{1_i}) \sum_{j\in\mathcal{V}} \beta_{0_{ji}} R_j,$$
$$\dot{A}_i = \alpha_i S_{0_i}(\sum_{j\in\mathcal{V}} \beta_{0_{ji}} R_j + \sum_{j\in\mathcal{V}} \beta_{1_{ji}} A_j).$$

このような系において，ネットワークの形状や攻撃者の位置がブロック拡散速度に与える影響を解明する．

(3) Bitcoin 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とその対策手法の検討

前述の SIRA モデルは，Bitcoin システムを含む，より一般的な競争的情報拡散システムにおける拡散妨害リスクをモデル化している一方，モデル化の前提において，Bitcoin システムならではの複雑な仕組みまでは考慮できていない．そこで本研究では，実際の Bitcoin プロトコルを考慮したシミュレーション評価により，Bitcoin ネットワークにおけるブロック拡散妨害攻撃のリスクを定量的に明らかにする．

さらに，拡散妨害攻撃への対策として，攻撃受信時の早期復旧と過去の経験に基づく攻撃回避について検討する（図 1 右）．前者に関しては，拡散妨害攻撃を完全に防ぐことは困難であり，万一，攻撃を受けたとしても早期に復旧する必要がある．具体的には，正規のブロック取得をできる限り阻害せずに攻撃の早期検知を可能とするタイムアウト制御方式を提案する．一方，後者に関しては，ブロック生成・拡散が継続的に行われる点に着目し，隣接ノードごとの過去の通信履歴を基に，将来の正常かつ迅速なブロック取得が期待できるノードを将来のブロック取得先ノードとして選択する方式を確立する．実際の Bitcoin ネットワークの構造を考慮したシミュレーション評価により，両方式による拡散妨害リスクの軽減効果を明らかにする．

４．研究成果

(1) Scalar SIRA モデルに基づく拡散妨害リスクの基本特性分析

Scalar SIRA モデルにおいて，前述のパラメタ $\alpha, \beta_0, \beta_1, \delta$ を変化させた場合における，情報拡散妨害リスクを定量的に評価する．システム内には，1 台の送信元ノード，$(1-\alpha)(N-1)$ 台の通常ノード，$\alpha(N-1)$ 台の攻撃者，計 1 万台 $(N = 1000)$ のノードが存在するものとする．時刻 $t = 0$ において，送信元ノードが新たな情報（ブロック）を生成したとし，その後のブロック拡散とその妨害の様子に着目する．以降の評価における各パラメタのデフォルト値を示す．図 2 における処理フローにおいて，最大 1 MB のブロックサイズ，実ネットワークにおける物理リンクの伝搬遅延時間，速度などを考慮し，ブロック伝播速度を $\beta_0 = 1$，攻撃速度を $\beta_1 = 10$ とする．また，$t_{\mathrm{TO}} \geq t_{\mathrm{bprop}}$ より，復帰速度を上限の $\delta = t_{\mathrm{TO}}^{-1} = 1$ とする．なお，実際の Bitcoin プロトコルでは $t_{\mathrm{TO}} = 600\,\mathrm{s}$ となり，その場合の復帰速度 $\delta = 0.00167$ は $\beta_0 = 1$ と比べて非常に遅く，よりリスクが高まる．また，単位時間あたりの他端末との通信頻度 cN を 8 とする．

図 4 に，Scalar SIRA モデルの時間推移を示す．図より，情報を取得できたノードの割合 R/N は急激にあるレベルまで上昇した後，緩やかに合意形成の状態へと推移することがわかる．一方，攻撃可能なノードの割合 A/N に関しても，急激な上昇の後，$\alpha = 0.01$ に収束していることがわかる．攻撃を受けたノードの割合 I/N に関しては，初期の時点では攻撃可能なノードの割合に合わせて上昇した後，復旧に伴い徐々に減衰していることがわかる．

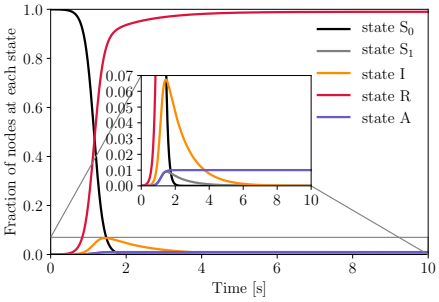


図 4: Scalar SIRA モデルの時間推移

図 5 に，攻撃者の割合 α を [0.0.05] の範囲で変化させた場合における，情報を取得できたノードの割合を示す．攻撃者が存在しない場合 $(\alpha = 0)$，通常の情報拡散は約 2 秒程度で合意形成に成功している．また，α の増加は，情報を取得したノード割合の初期の増加速度に対する影響は限定的である一方，その後の拡散速度を低下させる傾向が確認できる．

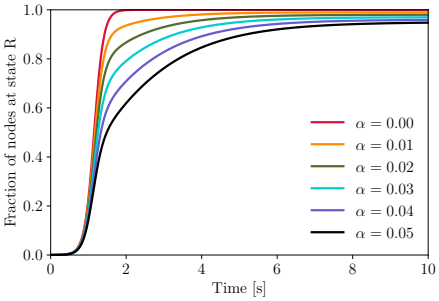


図 5: 攻撃者の割合 α による影響

その他，攻撃速度 β_1 や復旧速度 δ に関するリスク評価に関しては研究業績 [3] を参照のこと．

(2) Network SIRA モデルに基づくネットワーク構造を考慮した拡散妨害リスクの分析

Network SIRA モデルを用いることで，ネットワークの構造や送信元・攻撃者の位置が拡散妨害リスクに与える影響を評価する．評価においては，前述の Scalar SIRA モデルにおける設定を基に，ネットワークモデルとして，正則グラフ（均質な構造）と BA モデル [4] に基づくスケールフリーネットワーク（不均質な構造）を用いる．ただし比較のため，いずれのネットワークモデルにおいても平均次数が約 8 となるように設定する．

図 6 に，正則グラフとスケールフリーネットワークにおいて，送信元ノードと攻撃者をランダムに配置した場合における，情報取得ノードの割合の推移を示す．なお比較のため，Scalar SIRA モデルの結果を合わせて示す．

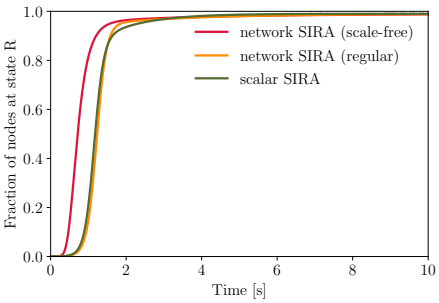


図 6: ネットワークの形状による影響

図より，正則グラフ上の Network SIRA モデルは Scalar SIRA モデルと似た挙動を示している．一方，スケールフリーネットワーク上の Network SIRA モデルは，高い次数を持つ通常ノードの存在により，拡散速度が向上していることがわかる．ただし，不均質なスケールフリーネットワークにおいては，送信元ノードと攻撃者の位置が拡散妨害リスクに影響を与えると考えられる．図 7 では，送信元ノードと攻撃者の位置として，前述のランダム配置に加えて，それぞれが高次数ノードとなる場合との比較結果を示している．図より，攻撃者が高次数ノードとなった場合，急激に拡散妨害リスクが増加することが確認できる．

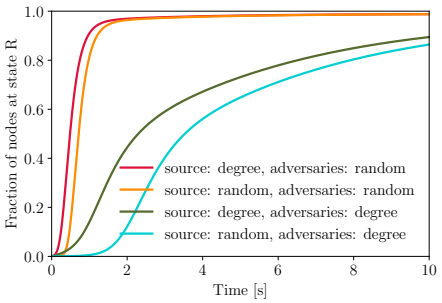


図 7: ブロック送信元・攻撃者の位置による影響

(3) Bitcoin 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とその対策手法の効果

以降では，評価結果の概要のみを示しており，詳細については研究業績 [5] を参照されたい．Bitcoin システムでは，新規ブロックの生成・拡散は平均 10 分の間隔で継続的に行われる．この評価では，システム内のノード間でブロックチェーンに対する合意が形成された，ある時刻 t_1 において，あるマイナーで新規のブロック b_1 が生成されたとみなし，b_1 のネットワーク上での拡散と攻撃者による妨害の様子に着目する．以降のブロック b_l $(l \geq 2)$ に対する生成時刻 t_l は，$t_l - t_{l-1}$ が平均 10 分の指数分布に従うものとする．ここで，各ブロック b_l は次のブロック b_{l+1} の生成時刻 t_{l+1} までに他のノードからの合意を得る必要がある．

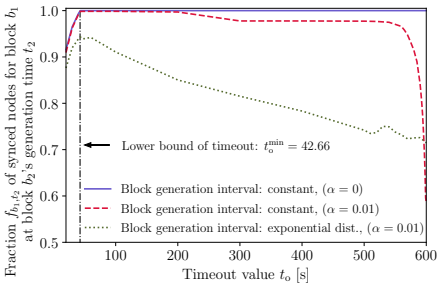


図 8: タイムアウト時間とブロック取得ノード割合の関係

図 8 に，タイムアウト時間 t_o と b_2 の生成時刻 t_2 における b_1 に対する取得ノード割合 f_{b_1,t_2} の関係を示す．図では，攻撃者の割合 α を 0.01 とした場合の結果を示しており，簡易な解析により導出されたタイムアウト時間 $t_o^{\min}$ 付近の値に t_o を設定することで f_{b_1,t_2} を向上できることを示している．また，ブロックの生成間隔が一定の場合や攻撃者が存在しない場合の結果を合わせて示しており，それらに比べてタイムアウト時間の設定がより重要となることがわかる．

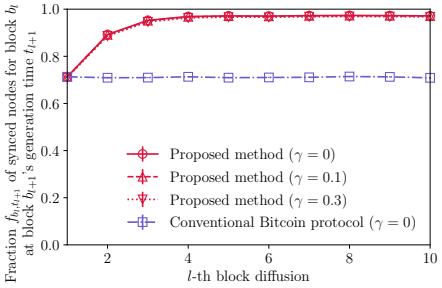


図 9: 取得先ノード選択方式とブロック取得ノード割合の関係

次に，図 9 に，l 回目 $(l = 1, \ldots, 10)$ のブロック拡散における，取得先ノード選択方式と b_{l+1} の生成時刻 t_{l+1} における b_l に対する取得ノード割合 $f_{b_l,t_{l+1}}$ の関係を示す．取得先選択方式では，隣接ノードごとの過去の通信時における受信レートの履歴情報から将来の受信レートを指数移動平均により予測する．$\gamma \geq 0$ は，隣接ノード間の通信速度に対する変動の程度を表すパラメタであり，図より，Bitcoin プロトコル本来の取得先選択方式と比較して，提案方式を用いることで，ブロック拡散の回数が進む毎に，γ の値によらず，攻撃を回避できていることがわかる．

参考文献

[1] A. Gervais, H. Ritzdorf, G. O. Karame, and S. Capkun, “Tampering with the Delivery of Blocks and Transactions in Bitcoin,” in *Proc. of ACM SIGSAC CCS’15*, 2015, pp. 692–705.

[2] C. Nowzari, V. M. Preciado, and G. J. Pappas, “Analysis and Control of Epidemics: A Survey of Spreading Processes on Complex Networks,” *IEEE Control Systems Magazine*, vol. 36, no. 1, pp. 26–46, 2016.

[3] M. Sasabe, “Mathematical Epidemiological Analysis of Dynamics of Delay Attacks on Pull-based Competitive Information Diffusion,” *Computer Networks*, vol. 180, pp. 1–9, Oct. 2020.

[4] A.-L. Barabási and R. Albert, “Emergence of Scaling in Random Networks,” *Science*, vol. 286, no. 5439, pp. 509–512, Oct. 1999.

[5] M. Sasabe, M. Yamamoto, Y. Zhang, and S. Kasahara, “Block Diffusion Delay Attack and Its Countermeasures in a Bitcoin Network,” *International Journal of Network Management*, vol. 32, no. 3, pp. 1–21, May 2022.

５．主な発表論文等

〔雑誌論文〕　計2件（うち査読付論文　2件／うち国際共著　0件／うちオープンアクセス　0件）

１．著者名 Sasabe Masahiro	４．巻 180
２．論文標題 Mathematical epidemiological analysis of dynamics of delay attacks on pull-based competitive information diffusion	５．発行年 2020年
３．雑誌名 Computer Networks	６．最初と最後の頁 107383:1～9
掲載論文のDOI（デジタルオブジェクト識別子） 10.1016/j.comnet.2020.107383	査読の有無 有
オープンアクセス オープンアクセスではない、又はオープンアクセスが困難	国際共著 －

１．著者名 Sasabe Masahiro、Yamamoto Masanari、Zhang Yuanyu、Kasahara Shoji	４．巻 32
２．論文標題 Block diffusion delay attack and its countermeasures in a Bitcoin network	５．発行年 2021年
３．雑誌名 International Journal of Network Management	６．最初と最後の頁 1-21
掲載論文のDOI（デジタルオブジェクト識別子） 10.1002/nem.2190	査読の有無 有
オープンアクセス オープンアクセスではない、又はオープンアクセスが困難	国際共著 －

〔学会発表〕　計5件（うち招待講演　1件／うち国際学会　1件）

１．発表者名 Masahiro Sasabe
２．発表標題 Interruption Risk of Competitive Block Diffusion in a Bitcoin Network
３．学会等名 Workshop on Internet Architecture and Applications（招待講演）（国際学会）
４．発表年 2019年

１．発表者名 笹部 昌弘
２．発表標題 Bitcoinネットワークにおけるブロック拡散妨害の数理モデル化
３．学会等名 電子情報通信学会ネットワークシステム研究会
４．発表年 2019年

１．発表者名 笹部 昌弘
２．発表標題 Bitcoinネットワークにおけるブロック拡散妨害の感染症伝播モデルに着想を得た数理モデル化
３．学会等名 超知性ネットワーキングに関する分野横断型研究会
４．発表年 2019年

１．発表者名 山本 将成，笹部 昌弘，笠原 正治
２．発表標題 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
３．学会等名 電子情報通信学会コミュニケーションクオリティ研究会
４．発表年 2019年

１．発表者名 山本 将成，笹部 昌弘，笠原 正治
２．発表標題 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への対抗策 ～ 推定ダウンロード速度に基づくブロック取得先選択 ～
３．学会等名 電子情報通信学会ネットワークシステム研究会
４．発表年 2020年

〔図書〕　計0件

〔産業財産権〕

〔その他〕

―

６．研究組織

	氏名 （ローマ字氏名） （研究者番号）	所属研究機関・部局・職 （機関番号）	備考

７．科研費を使用して開催した国際研究集会

〔国際研究集会〕　計0件

８．本研究に関連して実施した国際共同研究の実施状況

共同研究相手国	相手方研究機関