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　５ 年　 ６ 月 １９ 日現在

機関番号：１４６０３
研究種目：基盤研究(A)（一般）
研究期間：2019～2022
課題番号：１９Ｈ０１１０３

研究課題名（和文）超スケーラブル汎用ブロック・チェーン技術に向けた情報学的研究

研究課題名（英文）Informatics Study on Ultra-Scalable Blockchain Technology

研究代表者
笠原　正治（Kasahara, Shoji）

奈良先端科学技術大学院大学・先端科学技術研究科・教授

研究者番号：２０２６３１３９

交付決定額（研究期間全体）：（直接経費）　　38,760,000円

研究成果の概要（和文）：本研究課題では，ブロック・チェーンのセキュリティ・メカニズムについて，ネットワーク及び合意形成メカニズムの観点から数理的・実験的に性質を明らかにするとともに，近年着目されている分散台帳のデータ構造である有向非巡回グラフに対する特徴量を定義して理論的性質を明らかにした．また，ブロック・チェーンを基にした大規模IoTネットワーク用アクセス制御として属性ベースや能力ベースのアクセス制御方式を提案し，実証実験を通して提案手法の有効性を確認した．

研究成果の学術的意義や社会的意義
ブロック・チェーン技術では，分散性・安全性・拡張性の三点が重要な性質であるが，どのような種類のブロック・チェーンでも高々二つの性質しか満足できないトリレンマ問題が知られている．本研究課題では，参加者のインセンティブ，合意形成メカニズム，トランザクション処理性能の観点からトリレンマ問題の特徴を分析するとともに，ブロック・チェーン技術のIoT応用の上で重要な高度なセキュリティ保証と低コスト化を実現する方法論を検討したものであり，ブロック・チェーン技術の今後の発展に寄与する点は少なくない．

研究成果の概要（英文）：In this research project, we aimed to mathematically and experimentally investigate the security mechanisms of blockchain from the perspectives of network technologies and consensus mechanisms. We also proposed a characteristic feature for directed acyclic graphs (DAGs), a data structure of distributed ledgers that has gained attention in recent years, and clarified their theoretical properties. Furthermore, we proposed attribute-based and capability-based access control methods for large-scale IoT networks based on blockchain and confirmed the effectiveness of our proposed approach through empirical experiments.

研究分野：情報ネットワーク

キーワード：ブロック・チェーン　DSSトリレンマ　インセンティブ・メカニズム　セキュリティ　IoTアクセス制御

様　式　Ｃ－１９、Ｆ－１９－１、Ｚ－１９（共通）

１．研究開始当初の背景

インターネットやセンサー技術の急速な発展を背景に，従来のPCやタブレット・スマートフォン等の携帯端末に加えて，家電や自動車，ビルディングや工場など，多種多様なモノがインターネットにつながるIoT社会が到来しつつある．そのため，ネットワーク接続された莫大な数のIoT機器に対する高度なセキュリティ保証技術の開発が急務となっており，解決技術の一つとしてブロック・チェーンを活用するアプローチが注目されている．

莫大な数のIoT端末から構成されるIoTシステムでは，取り扱う情報の種類と量は時間的・空間的に膨大であり，そのためIoT用ブロック・チェーンには高速なトランザクション処理と高いスケーラビリティが欠かせない．しかしながら，ビットコインやイーサリアムのブロック・チェーン技術では，不特定多数の参加ノード間のハッシュ計算競争（マイニング）に基づくプルーフ・オブ・ワーク(Proof-of-Work: PoW)と呼ばれる合意形成処理とブロックサイズがボトルネックとなり，単位時間当たりのトランザクション処理量は極めて少ないスケーラビリティの問題がある．高スケーラビリティの実現にはマイニングに代表される合意形成処理時間を短縮することが必須であるが，合意形成処理時間を短縮すると，ある承認ブロックがP2Pネットワーク上の全参加ノードにブロードキャストされる間に，別ノードでブロックが承認されてチェーンが分岐するフォークと呼ばれる現象が頻発する．フォークが多発する状況では，悪意あるユーザが不正ブロックをチェーンに接続する危険性が高くなるため，分岐チェーンの正当性判断がブロック・チェーンの真正性を保証する上で重要となる．

２．研究の目的

ブロック・チェーンを特徴づける重要要素は，分散性・安全性・拡張性（スケーラビリティ）の三点である．ビットコインに代表されるパブリック型ブロック・チェーンは，安全性と分散性の二つを満足している一方でトランザクション処理速度が著しく低く，スケーラビリティに問題がある．一方，フィンテック応用で注目を集めているプライベート型やコンソーシアム型のブロック・チェーンは，中央集権型組織が承認したノードのみブロック・チェーンを管理できる参加ノード限定型技術であり，分散性を犠牲にする代わりに高い安全性と高スケーラビリティを実現している．つまり，分散性とスケーラビリティの二つはセキュリティを介して相反関係にあり（DSS トリレンマと呼ばれる），合意形成処理時間の短縮が脆弱なセキュリティを誘発することからもわかるように，三要素すべてを満足するブロック・チェーンを実現することは極めて困難であることに注意する．本研究課題では，ブロック・チェーンの DSS トリレンマの問題の本質を数理的・実験的に明らかにし，情報量が圧縮されかつ高速演算可能な先進的データ構造を検討するとともに，大規模 IoT ネットワークに適用可能なブロック・チェーン応用技術について研究開発を行った．

３．研究の方法

(1) ブロック・チェーンにおけるセキュリティ・メカニズムの解明

本研究の基礎的検討として，合意形成アルゴリズムと P2P ネットワークの特性がセキュリティ強度に与える影響を，数理的分析と大規模シミュレーション実験により定量的かつ多角的に分析を行う．具体的には，トランザクション承認過程やユーザ・マイナーの行動をマルコフ過程等の確率過程やゲーム理論でモデル化し，トランザクションの到着過程やブロックの接続方法と，悪意あるユーザのブロック乗っ取り成功確率といったセキュリティ脆弱性指標の間のトレードオフ分析を通じて主要パラメータと評価指標の相関構造を定量的・定性的に把握し，合意形成アルゴリズムの改善に向けた知見を得ることを目指した．

(2) ブロック・チェーンに向けた高速処理可能な先進的データ構造の確立

近年IoT応用を目指して開発が進められているIOTAでは有向非巡回グラフ(Directed Acyclic Graph: DAG)に従う Tangle が採用されており，そこではトランザクション生成ノードが未承認状態でチェーンに接続されているトランザクションの承認処理を行うことで，省力型の承認処理を実現している．一方で，トランザクション高負荷時にはフォークが多発し，全参加ノードでブロック・チェーンを確実に同期することができないという致命的な欠点がある．ここではDAGに対する計算処理に有効な測度の導入と理論的性質について検討を行った．

(3) 高度なセキュリティを保証する IoT アクセス制御

研究代表者の研究組織では過去にイーサリアムのスマート・コントラクトを応用した IoT アクセス制御方式を提案し，2 台の RaspberryPi3 と PC2 台からなる実験システムを構築して実証実験を行った．本課題でも上述の汎用ブロック・チェーンの実証実験に向けた実機システムの開発を並行して行った．具体的には，P2P ピアノード，IoT デバイスから構成される実験システムを構築し，属性ベースや能力ベースのアクセスを提供するスマート・コントラクトの開発等，IoT アクセス制御方式の機能拡張も推進した．

４．研究成果

(1) セキュリティメカニズム

① ビットコインにおけるブロック拡散プロトコルの脆弱性分析

ビットコインでは，システムに参加するノード間で P2P ネットワーク（ビットコインネットワーク）を構築し，取引情報やその集まりであるブロックをやりとりし，取引台帳を分散的にブロックチェーンとして保有する．このとき，ネットワーク上での速やかなブロックの拡散は，ブロック・チェーンに対するノード間での合意形成に欠かせない．一方で，ビットコイン・クライアントはオープンソースで開発されており，悪意のあるノードが改変することも可能である．先行研究では，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攻撃者が悪用することで，隣接ノードに対するブロックの伝搬を遅らせるブロック伝搬遅延攻撃が指摘されている[1, 2]．

ここでは，特定のマイナーノードが複数の攻撃者と結託して競合するマイナーの生成ブロックの拡散を妨害するブロック拡散妨害攻撃に着目し，計算機シミュレーションによってブロック拡散妨害攻撃の基本特性について評価を行った．図 1 は攻撃者の配置がランダムのときのブロック取得ノードの割合の推移を示している．この図より，攻撃者が存在しない場合（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があることに注意する．

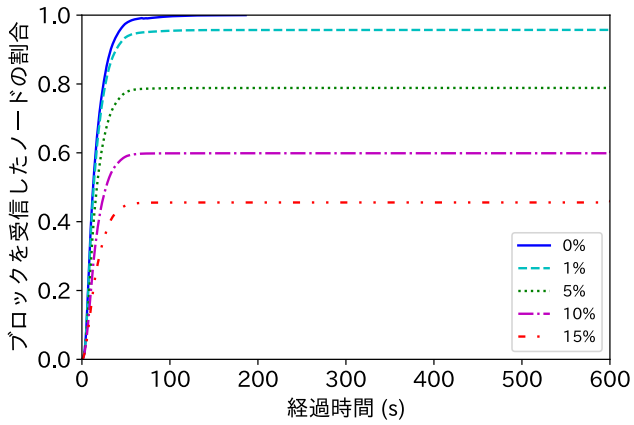


図 1：攻撃者の割合とブロック取得ノードの割合（攻撃者の配置：ランダム）

② PoS 型コンセンサスアルゴリズムにおけるインセンティブ・メカニズム

ブロック・チェーンの代表的なコンセンサス・アルゴリズムである Proof-of-Work (PoW) では，ブロック承認のために大量の電力が消費されることが欠点として知られている．PoW の欠点を改良するためのコンセンサス・アルゴリズムとして，計算能力をそれほど必要としない Proof-of-Stake (PoS) が提案されている．PoS では，PoW における計算力を Stake と呼ばれる仮想通貨で支払われる保証金で代替する．PoW では高い計算能力を持つノードがブロックを生成する権利を獲得するが，PoS では参加ノードは保有する Stake の量に応じてブロックを生成する権利を獲得する．ここでは，正しい投票を行う動機付けをバリデータに対して行うための報酬・罰則付与型 PoS コンセンサス・アルゴリズムについて基本的検討を行った．具体的には，バリデータの過去の投票履歴から投票信頼度を計算し，投票信頼度を基に投票結果に対する報酬罰則メカニズムを提案した．計算機シミュレーションにより，信頼度の推定は投票行動に追従して妥当な信頼度の値を提供できることを確認した．また，罰則の重みを大きくするほど，正しい投票をしないバリデータに対して厳しい罰を課すことを確認した．あまりにも厳しい罰則を課してしまうと，バリデータがシステムから離脱し，PoS による合意形成が機能しなくなる恐れがあるため，罰則の重みパラメータについては慎重な設計が必要である．

③ 手数料・承認遅延・セキュリティを考慮したインセンティブ・メカニズム解析

ビットコイン型ブロック・チェーンでは，高い手数料が付与されたトランザクションほど早くブロックに含められる優先処理がマイナーノードによって行われている．そのため，エンドユーザにとっては許容範囲の遅延でトランザクションが処理されるのに必要な手数料に興味がある．マイナーは収益を増やすために高い手数料を含むトランザクションをブロックに含めることに興味がある．ブロックサイズの増大はブロック承認処理やネットワーク伝搬遅延を増大させる傾向にあり，エンドユーザの効用を減少させるだけでなく，フォークの多発による脆弱なセキュリティ状況になる恐れがある[3, 4]．このようなトランザクション手数料，承認処理遅延，セキュリティの三要素の依存関係を表現する数理モデルを考え，その妥当性について検証を行った．具体的には，承認処理遅延については待ち行列理論を応用した確率モデルを構築し，手数料・報酬及びセキュリティについてはユ

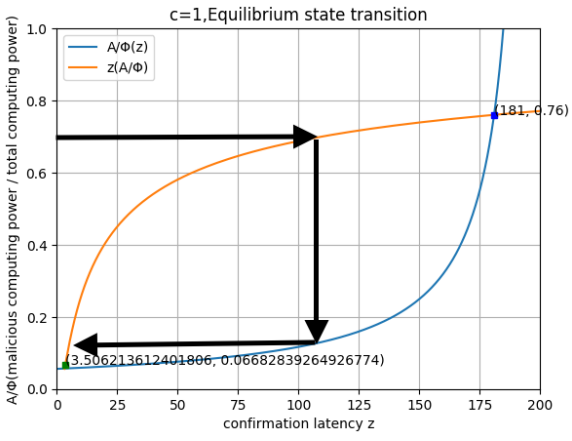


図 2：遅延と計算パワーにおける均衡点の推移

ーザ及びマイナーの効用に対するナッシュ均衡分析を行い，系のナッシュ均衡解がどのように推移するかを計算機シミュレーションにより評価を行った．数値実験を通して，提案した数理モデルにより，トランザクションの承認遅延，手数料，セキュリティの 3 要素がどのように依存して系が推移するかを定量的に評価できることが確認された．（図 2 参照）

(2) 先進的データ構造：DAG に対する幅とアルゴリズム

グラフに対する計算処理を効率よく行うため，グラフの特性を表す指標を考え，その指標を用いてアルゴリズムを設計することがある．無向グラフにおいては，パスへの類似度を表すパス幅[5]や木への類似度を表す木幅[6, 7]といった幅の指標が知られており，この幅が小さいときにある種の問題を効率的に解く手法がいくつか知られている．有向グラフにおいても Directed-path-width[8]といった手法が知られており，これらは有向非巡回グラフ(DAG)への類似度を表すものに近い．しかしながら，DAG に対する幅の指標はこれまで研究されてこなかった．ここでは幅が小さい DAG 上のある種の問題を効率的に解くことを検討した．具体的には，DAG に対する幅の指標として有向パス幅を無向グラフにおけるパス幅の拡張として定義した．次に有向パス幅の小さい DAG 上の問題を効率的に解くアルゴリズムを設計した．アルゴリズムの一例として，DAG $D=(V,E)$を入力として，各頂点について到達可能な頂点数を出力する問題を考える．愚直な全探索では$O(|V||E|)$時間で計算することができる．これより高速な解法も知られているが，いずれも$\Omega(|V|^2)$時間必要である．ここで入力に DAG $D$ に加え，幅 $W$ の DAG パス分解 $X=(X_1,X_2,\dots,X_s)$が与えられるとする．このとき$O(2^W W^2|V|)$時間で計算することができる．すなわち，幅$W$が定数のとき，頂点数に対して線形時間で計算することができる．

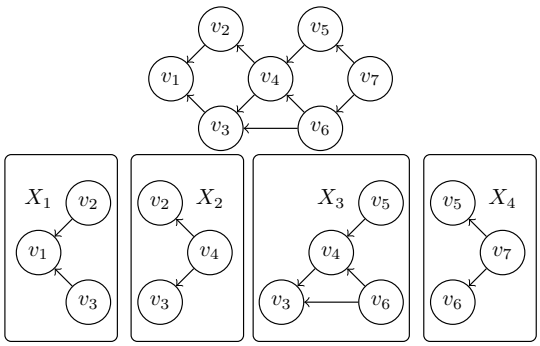

図 3：DAG パス分解の例

図 3 を用いて計算方法を説明する．例として，$X_4$に含まれる$v_7$について注目する．$v_7$ から到達できる $X_1$，$X_2$，$X_3$の頂点数は$X_3$と$X_4$の共通部分である$v_5$または$v_6$を通る．これは（$v_5$から到達でき，$v_6$からは到達できない頂点数)+($v_5$から到達できず，$v_6$からは到達できる頂点数)+($v_5$と$v_6$から到達できる頂点数） によって計算できる．このアイデアを一般化すると，$i=1,2,\dots,s$と順に各$X_i$とその部分集合$A$について$A$の全ての頂点から到達でき，$X_i \setminus A$のどの頂点からも到達できない頂点数を計算していくことで，各頂点から到達可能な頂点数を計算することができる．

(3) IoT アクセス制御技術

大規模 IoT ネットワークに対し，耐改ざん性に優れた分散型データベースであるブロック・チェーンを用いたアクセス制御が考えられている[9, 10]．ここでは Ethereum のスマートコントラクトを用いて，サブジェクトに対する権限付与の方法として Capability と属性の 2 種類のアクセス制御方式を検討した．また，IoT 応用に特化した IOTA ベースのアクセス制御方式についても検討を行った．

① Capability アクセス制御方式

ここでは，Capability 情報の整合性を保つために一つの権限と譲渡関係を結びつけたトークンによる権限管理，及び Capability の単位をアクション単位で行う管理手法を提案した．提案手法ではオブジェクトに対して新しいアクションの追加・削除を行う機能も実現した．提案手法の実行可能性を検証するため，実機による実証実験を行った．権限管理機能の動作実験，及び権限検証の動作実験を行い，提案手法がオブジェクト毎にアクション単位で Capability を構築・管理できることを確認した．

② 属性ベース・アクセス制御方式

我々の過去の研究成果として，スマートコントラクトを用いて，属性ベースのアクセス制御(Attribute-Based Access Control: ABAC)を実現した．そこではアクセス制御ポリシーはそれを記述したページへの URL リンクとしてブロック・チェーンに格納されるため，ブロック・チェーンの肥大化を防ぐことを可能とした．しかしながら，ポリシー自体をブロック・チェーン内で管理していないため，URL 先で管理されているポリシーの改ざんリスクが問題であった．また，サブジェクトやオブジェクトの属性情報をブロック・チェーンで管理していないため，属性情報の信頼性も不十分であった．ここではこれらの問題点を解決するための Ethereum ブロック・チェーンのスマートコントラクトを用いた分散型 ABAC を検討した．（図 4 参照.）提案手法の動作を確認するため，1 台の計算機サーバ上に 3 台の仮想 Ethereum ノードからなるプライベート・ブロック・チェーン・ネットワークを構築し，実証実験を行った．実証実験において，ブロック・チェーン上に保存されているサブジェクト・オブジェクト属性情報を取得し，対応するポリシーを検索して要求操作

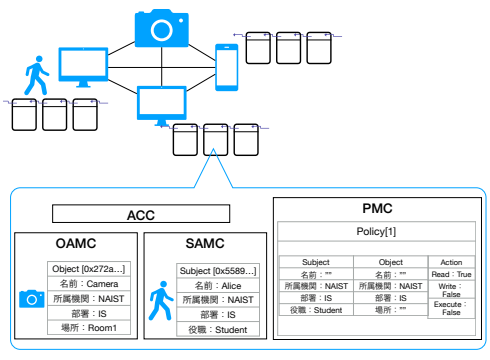

図 4：ABAC 提案方式

を認可する，という一連の動作を確認できた．また提案手法の性能評価として，スマートコントラクトの展開や ABI の実行時に支払われる Gas を計測し，提案手法では Gas 消費量が既存手法と比べて増大すること，一方でサブジェクトとオブジェクトの増加に対して提案手法は ACC やポリシーの登録数を抑えることができることを確認した．

③ IOTA 分散台帳を利用した IoT アクセス制御方式

IOTA[11]は Machine-to-Machine (M2M)の少額決済に特化した分散台帳技術である．Bitcoin や Ethereum とは異なり，IOTA の分散台帳である Tangle は有向非巡回グラフ (Directed Acyclic Graph: DAG) になっている．IOTA にはスマートコントラクトは実装されていないものの，Masked Authenticated Messaging (MAM)[12]と呼ばれるデータ通信プロトコルがあり，改ざんが困難な形で Tangle に対するデータの記録・参照を行うことができる．IOTA ベースのアクセス制御に関する関連研究[13]では，DCACI と呼ばれる MAM を用いた分散型能力ベースのアクセス制御が提案されている．DCACI では，サブジェクトはまずオブジェクトを管理するドメイン所有者にリクエストを送信する．ドメイン所有者はサブジェクトを認証した上で与える権限の決定とトークンの発行を行い，トークンをサブジェクトに送信すると同時に MAM を用いて自身のメッセージチャネルに原本を記録する．アクセスの際には，サブジェクトはアクセスリクエストとともにトークンをドメイン所有者に提示する．ドメイン所有者は提示されたトークンを Tangle に記録された原本と照合し，トークンの真正性・有効性に基づいてアクセスの可否を決定する．

DCACI では IOTA を利用することで手数料のかからない分散型アクセス制御が実現されているものの，ドメイン所有者とサブジェクトとの間に安全な通信路の存在や適切な認証が行われることを前提としており，また一対一のアクセス制御しか行うことができない．加えて権限付与の方法が明確に定められていないといった欠点がある．ここではこれらの問題点を克服するため，IOTA に属性ベース暗号技術である Ciphertext-Policy Attribute-Based Encryption (CP-ABE)を組み合わせる方式を検討した．図 5 は提案手法の処理の流れを示している． 提案手法の実現可能性を示すため，プロトタイプの実装を行い，実際の IOTA ネットワークである Devnet を用いて実証実験を行った．実証実験を通じてドメイン所有者側のトークン発行と CP-ABE による暗号化，権限検証が動作することを確認した．

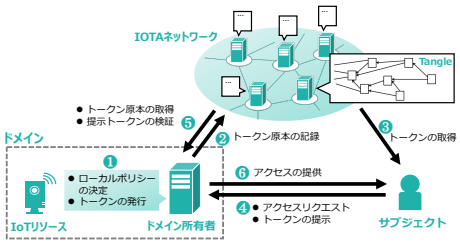


図 5：DCACI と MAM を用いた提案方式

参考文献

[1] T. Neudecker and H. Hartenstein, “Network Layer Aspects of Permissionless Blockchains,” IEEE Communications Surveys and Tutorials, vol.21, no.1, pp.838-857, 2019.
[2] 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.
[3] J. He, G. Zhang, J. Zhang, and R. Zhang, “An economic model of blockchain: The interplay between transaction fees and security,” Available at SSRN 3616869, 2020.
[4] G. Huberman, J.D. Leshno, and C. Moallemi, “Monopoly without a monopolist: An economic analysis of the bitcoin payment system,” The Review of Economic Studies, Vol. 88, No. 6, pp. 3011-3040, 2021.
[5] N. Robertson and P. Seymour, “Graph minors. I. Excluding a forest,” Journal of Combinatorial Theory, Series B, Vol. 35, No. 1, pp. 39-61, 1983.
[6] R. Halin, “S-functions for graphs,” Journal of Geometry, Vol. 8, No. 1, pp. 171-186, 1976.
[7] N. Robertson and P. Seymour, “Graph minors. III. Planar tree-width,” Journal of Combinatorial Theory, Series B, Vol. 36, No. 1, pp. 49-64, 1984.
[8] B.A. Reed, “Tree width and tangles: a new connectivity measure and some applications,” Surveys in Combinatorics, pp. 87-162, 1997.
[9] D.D.M. Francesco, P. Mori, and L. Ricci, “Blockchain based access control,” Proc. of IFIP International Conference on Distributed Applications and Interoperable Systems, pp.206-220, May 2017.
[10] A. Ouaddah, A.A. Elkalam, and A.A. Ouahman, “FairAccess: a new blockchain-based access control framework for the Internet of Things,” Security and Communication Networks, vol.9, pp.5943-5964, Feb. 2017.
[11] “The Next Generation of Distributed Ledger Technology IOTA,” Available at https://www.iota.org/.
[12] J. Bethencourt, A. Sahai and B. Waters, “Ciphertext-Policy Attribute-Based Encryption,” Proc. of the 2007 IEEE Symposium on Security and Privacy, pp.321-334, 2007.
[13] S. K. Pinjala and K. M. Sivalingam, “DCACI: A Decentralized Lightweight Capability Based Access Control Framework using IOTA for Internet of Things,” The Fourth IEEE International Workshop on Security and Privacy for Internet of Things and Cyber-Physical Systems, pp.13-18, 2019.

５．主な発表論文等

〔雑誌論文〕　計22件（うち査読付論文　22件／うち国際共著　6件／うちオープンアクセス　12件）

| | |
|---|---|
| １．著者名<br>Hiraide Takumi、Kasahara Shoji | ４．巻<br>6 |
| ２．論文標題<br>Analysis of interaction between miner decision making and user action for incentive mechanism of bitcoin blockchain | ５．発行年<br>2023年 |
| ３．雑誌名<br>Frontiers in Blockchain | ６．最初と最後の頁<br>- |
| 掲載論文のDOI（デジタルオブジェクト識別子）<br>10.3389/fbloc.2023.1067628 | 査読の有無<br>有 |
| オープンアクセス<br>オープンアクセスとしている（また、その予定である） | 国際共著<br>－ |

| | |
|---|---|
| １．著者名<br>KASAHARA Shoji、KAWAHARA Jun、MINATO Shin-ichi、MORI Jumpei | ４．巻<br>E106.D |
| ２．論文標題<br>DAG-Pathwidth: Graph Algorithmic Analyses of DAG-Type Blockchain Networks | ５．発行年<br>2023年 |
| ３．雑誌名<br>IEICE Transactions on Information and Systems | ６．最初と最後の頁<br>272～283 |
| 掲載論文のDOI（デジタルオブジェクト識別子）<br>10.1587/transinf.2022FCP0007 | 査読の有無<br>有 |
| オープンアクセス<br>オープンアクセスとしている（また、その予定である） | 国際共著<br>－ |


| | |
|---|---|
| １．著者名<br>Hiraide Takumi、Kasahara Shoji | ４．巻<br>6 |
| ２．論文標題<br>Analysis of interaction between miner decision making and user action for incentive mechanism of bitcoin blockchain | ５．発行年<br>2023年 |
| ３．雑誌名<br>Frontiers in Blockchain | ６．最初と最後の頁<br>- |
| 掲載論文のDOI（デジタルオブジェクト識別子）<br>10.3389/fbloc.2023.1067628 | 査読の有無<br>有 |
| オープンアクセス<br>オープンアクセスとしている（また、その予定である） | 国際共著<br>－ |

| | |
|---|---|
| １．著者名<br>KASAHARA Shoji、KAWAHARA Jun、MINATO Shin-ichi、MORI Jumpei | ４．巻<br>E106.D |
| ２．論文標題<br>DAG-Pathwidth: Graph Algorithmic Analyses of DAG-Type Blockchain Networks | ５．発行年<br>2023年 |
| ３．雑誌名<br>IEICE Transactions on Information and Systems | ６．最初と最後の頁<br>272～283 |
| 掲載論文のDOI（デジタルオブジェクト識別子）<br>10.1587/transinf.2022FCP0007 | 査読の有無<br>有 |
| オープンアクセス<br>オープンアクセスとしている（また、その予定である） | 国際共著<br>－ |

| | |
|---|---|
| 1．著者名<br>MATSUNAGA Takeaki、ZHANG Yuanyu、SASABE Masahiro、KASAHARA Shoji | 4．巻<br>E105.B |
| 2．論文標題<br>An Incentivization Mechanism with Validator Voting Profile in Proof-of-Stake-Based Blockchain | 5．発行年<br>2022年 |
| 3．雑誌名<br>IEICE Transactions on Communications | 6．最初と最後の頁<br>228～239 |
| 掲載論文のDOI（デジタルオブジェクト識別子）<br>10.1587/transcom.2021CEP0004 | 査読の有無<br>有 |
| オープンアクセス<br>オープンアクセスとしている（また、その予定である） | 国際共著<br>該当する |

| | |
|---|---|
| 1．著者名<br>KASAHARA Shoji | 4．巻<br>E104.B |
| 2．論文標題<br>Performance Modeling of Bitcoin Blockchain: Mining Mechanism and Transaction-Confirmation Process | 5．発行年<br>2021年 |
| 3．雑誌名<br>IEICE Transactions on Communications | 6．最初と最後の頁<br>1455～1464 |
| 掲載論文のDOI（デジタルオブジェクト識別子）<br>10.1587/transcom.2021ITI0003 | 査読の有無<br>有 |
| オープンアクセス<br>オープンアクセスとしている（また、その予定である） | 国際共著<br>－ |

| | |
|---|---|
| 1．著者名<br>Sasabe Masahiro、Yamamoto Masanari、Zhang Yuanyu、Kasahara Shoji | 4．巻<br>32 |
| 2．論文標題<br>Block diffusion delay attack and its countermeasures in a Bitcoin network | 5．発行年<br>2021年 |
| 3．雑誌名<br>International Journal of Network Management | 6．最初と最後の頁<br>- |
| 掲載論文のDOI（デジタルオブジェクト識別子）<br>10.1002/nem.2190 | 査読の有無<br>有 |
| オープンアクセス<br>オープンアクセスとしている（また、その予定である） | 国際共著<br>該当する |

| | |
|---|---|
| 1．著者名<br>Zhang Yuanyu、Nakanishi Ruka、Sasabe Masahiro、Kasahara Shoji | 4．巻<br>21 |
| 2．論文標題<br>Combining IOTA and Attribute-Based Encryption for Access Control in the Internet of Things | 5．発行年<br>2021年 |
| 3．雑誌名<br>Sensors | 6．最初と最後の頁<br>5053～5053 |
| 掲載論文のDOI（デジタルオブジェクト識別子）<br>10.3390/s21155053 | 査読の有無<br>有 |
| オープンアクセス<br>オープンアクセスとしている（また、その予定である） | 国際共著<br>該当する |

| | |
|---|---|
| 1．著者名<br>Zhang Yuanyu、Yutaka Mirei、Sasabe Masahiro、Kasahara Shoji | 4．巻<br>8 |
| 2．論文標題<br>Attribute-Based Access Control for Smart Cities: A Smart-Contract-Driven Framework | 5．発行年<br>2021年 |
| 3．雑誌名<br>IEEE Internet of Things Journal | 6．最初と最後の頁<br>6372～6384 |
| 掲載論文のDOI（デジタルオブジェクト識別子）<br>10.1109/JIOT.2020.3033434 | 査読の有無<br>有 |
| オープンアクセス<br>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<br>該当する |

| | |
|---|---|
| 1．著者名<br>Wiraatmaja Christopher、Zhang Yuanyu、Sasabe Masahiro、Kasahara Shoji | 4．巻<br>- |
| 2．論文標題<br>Cost-Efficient Blockchain-Based Access Control for the Internet of Things | 5．発行年<br>2021年 |
| 3．雑誌名<br>2021 IEEE Global Communications Conference (GLOBECOM) | 6．最初と最後の頁<br>- |
| 掲載論文のDOI（デジタルオブジェクト識別子）<br>10.1109/GLOBECOM46510.2021.9685205 | 査読の有無<br>有 |
| オープンアクセス<br>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<br>該当する |

| | |
|---|---|
| 1．著者名<br>Fujita Kentaro、Zhang Yuanyu、Sasabe Masahiro、Kasahara Shoji | 4．巻<br>- |
| 2．論文標題<br>Intelligent Mining Pool Selection in the Case of Unobservable Block Withholding Attack | 5．発行年<br>2021年 |
| 3．雑誌名<br>2021 IEEE International Conference on Blockchain and Cryptocurrency (ICBC 2021) | 6．最初と最後の頁<br>- |
| 掲載論文のDOI（デジタルオブジェクト識別子）<br>10.1109/ICBC51069.2021.9461125 | 査読の有無<br>有 |
| オープンアクセス<br>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<br>該当する |

| | |
|---|---|
| 1．著者名<br>Fujita Kentaro、Zhang Yuanyu、Sasabe Masahiro、Kasahara Shoji | 4．巻<br>11 |
| 2．論文標題<br>Mining Pool Selection under Block WithHolding Attack | 5．発行年<br>2021年 |
| 3．雑誌名<br>Applied Sciences | 6．最初と最後の頁<br>1617～1617 |
| 掲載論文のDOI（デジタルオブジェクト識別子）<br>10.3390/app11041617 | 査読の有無<br>有 |
| オープンアクセス<br>オープンアクセスとしている（また、その予定である） | 国際共著<br>－ |

| | |
|---|---|
| 1．著者名<br>Hara Takanori、Sasabe Masahiro、Kasahara Shoji | 4．巻<br>1 |
| 2．論文標題<br>Selfish Yet Optimal Routing by Adjusting Perceived Traffic Information of Road Networks | 5．発行年<br>2020年 |
| 3．雑誌名<br>IEEE Open Journal of Intelligent Transportation Systems | 6．最初と最後の頁<br>120～133 |
| 掲載論文のDOI（デジタルオブジェクト識別子）<br>10.1109/OJITS.2020.3019935 | 査読の有無<br>有 |
| オープンアクセス<br>オープンアクセスとしている（また、その予定である） | 国際共著<br>－ |

| | |
|---|---|
| 1．著者名<br>Hara Takanori、Sasabe Masahiro、Matsuda Taiki、Kasahara Shoji | 4．巻<br>9 |
| 2．論文標題<br>Capacitated Refuge Assignment for Speedy and Reliable Evacuation | 5．発行年<br>2020年 |
| 3．雑誌名<br>ISPRS International Journal of Geo-Information | 6．最初と最後の頁<br>442～442 |
| 掲載論文のDOI（デジタルオブジェクト識別子）<br>10.3390/ijgi9070442 | 査読の有無<br>有 |
| オープンアクセス<br>オープンアクセスとしている（また、その予定である） | 国際共著<br>－ |

| | |
|---|---|
| 1．著者名<br>Nishi Yohei、Sasabe Masahiro、Kasahara Shoji | 4．巻<br>13 |
| 2．論文標題<br>Optimality analysis of locality-aware tit-for-tat-based P2P file distribution | 5．発行年<br>2020年 |
| 3．雑誌名<br>Peer-to-Peer Networking and Applications | 6．最初と最後の頁<br>1688～1703 |
| 掲載論文のDOI（デジタルオブジェクト識別子）<br>10.1007/s12083-020-00925-2 | 査読の有無<br>有 |
| オープンアクセス<br>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<br>－ |

| | |
|---|---|
| 1．著者名<br>Qu Qianyue、Zhang Yuanyu、Kasahara Shoji | 4．巻<br>- |
| 2．論文標題<br>On Eavesdropping Region Characterization in Hybrid Wireless Communications | 5．発行年<br>2020年 |
| 3．雑誌名<br>2020 International Conference on Networking and Network Applications (NaNA2020) | 6．最初と最後の頁<br>29-34 |
| 掲載論文のDOI（デジタルオブジェクト識別子）<br>10.1109/NaNA51271.2020.00013 | 査読の有無<br>有 |
| オープンアクセス<br>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<br>－ |

| | |
|---|---|
| 1．著者名<br>Fujita Kentaro、Zhang Yuanyu、Sasabe Masahiro、Kasahara Shoji | 4．巻<br>- |
| 2．論文標題<br>Mining Pool Selection Problem in the Presence of Block Withholding Attack | 5．発行年<br>2020年 |
| 3．雑誌名<br>The 3rd IEEE International Conference on Blockchain (Blockchain-2020) | 6．最初と最後の頁<br>329-334 |
| 掲載論文のDOI（デジタルオブジェクト識別子）<br>10.1109/Blockchain50366.2020.00047 | 査読の有無<br>有 |
| オープンアクセス<br>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<br>－ |

| | |
|---|---|
| 1．著者名<br>Nakanishi Ruka、Zhang Yuanyu、Sasabe Masahiro、Kasahara Shoji | 4．巻<br>- |
| 2．論文標題<br>IOTA-Based Access Control Framework for the Internet of Things | 5．発行年<br>2020年 |
| 3．雑誌名<br>The 2nd conference on Blockchain Research and Applications for Innovative Networks and Services (BRAINS'20) | 6．最初と最後の頁<br>87-95 |
| 掲載論文のDOI（デジタルオブジェクト識別子）<br>10.1109/BRAINS49436.2020.9223293 | 査読の有無<br>有 |
| オープンアクセス<br>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<br>－ |

| | |
|---|---|
| 1．著者名<br>Nakamura Yuta、Zhang Yuanyu、Sasabe Masahiro、Kasahara Shoji | 4．巻<br>20 |
| 2．論文標題<br>Exploiting Smart Contracts for Capability-Based Access Control in the Internet of Things | 5．発行年<br>2020年 |
| 3．雑誌名<br>Sensors | 6．最初と最後の頁<br>1793～1793 |
| 掲載論文のDOI（デジタルオブジェクト識別子）<br>10.3390/s20061793 | 査読の有無<br>有 |
| オープンアクセス<br>オープンアクセスとしている（また、その予定である） | 国際共著<br>－ |

| | |
|---|---|
| 1．著者名<br>Nakamura Yuta、Zhang Yuanyu、Sasabe Masahiro、Kasahara Shoji | 4．巻<br>- |
| 2．論文標題<br>Capability-Based Access Control for the Internet of Things: An Ethereum Blockchain-Based Scheme | 5．発行年<br>2019年 |
| 3．雑誌名<br>IEEE GLOBECOM 2019 | 6．最初と最後の頁<br>- |
| 掲載論文のDOI（デジタルオブジェクト識別子）<br>10.1109/GLOBECOM38437.2019.9013321 | 査読の有無<br>有 |
| オープンアクセス<br>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<br>－ |

| | |
|---|---|
| 1．著者名<br>Yutaka Mirei、Zhang Yuanyu、Sasabe Masahiro、Kasahara Shoji | 4．巻<br>- |
| 2．論文標題<br>Using Ethereum Blockchain for Distributed Attribute-Based Access Control in the Internet of Things | 5．発行年<br>2019年 |
| 3．雑誌名<br>IEEE GLOBECOM 2019 | 6．最初と最後の頁<br>- |
| 掲載論文のDOI（デジタルオブジェクト識別子）<br>10.1109/GLOBECOM38437.2019.9014155 | 査読の有無<br>有 |
| オープンアクセス<br>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<br>－ |

| | |
|---|---|
| 1．著者名<br>Nishi Yohei、Sasabe Masahiro、Kasahara Shoji | 4．巻<br>- |
| 2．論文標題<br>Impact of Locality-awareness on Tit-for-Tat-based P2P File Distribution | 5．発行年<br>2020年 |
| 3．雑誌名<br>IEEE Consumer Communications & Networking Conference 2020 (IEEE CCNC 2020) | 6．最初と最後の頁<br>- |
| 掲載論文のDOI（デジタルオブジェクト識別子）<br>10.1109/CCNC46108.2020.9045338 | 査読の有無<br>有 |
| オープンアクセス<br>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<br>－ |

〔学会発表〕　計33件（うち招待講演　2件／うち国際学会　10件）

| |
|---|
| 1．発表者名<br>Hiraide Takumi, Kasahara Shoji |
| 2．発表標題<br>A Mathematical Model of Blockchains Considering 2022年度OR学会関西支部 若手研究発表会 of Fees, Confirmation Latency, and Security |
| 3．学会等名<br>2022 International Conference on Emerging Technologies for Communications (ICETC2022)（国際学会） |
| 4．発表年<br>2022年 |

| |
|---|
| 1．発表者名<br>杉原健斗，原崇徳，笹部昌弘，笠原正治 |
| 2．発表標題<br>VNFの多様性・冗長性に基づく可用性と資源効率を考慮したサービスチェイニングとVNF配置方式 |
| 3．学会等名<br>電子情報通信学会技術研究報告 (NS2022-167), pp. 1-6 |
| 4．発表年<br>2023年 |

１．発表者名
平出託海，笠原正治

２．発表標題
A mathematical model of user-miner interaction through confirmation latency and fees in Bitcoin-type blockchains

３．学会等名
第39回(2022年度)待ち行列シンポジウム「確率モデルとその応用」，早稲田大学本キャンパス小野記念講堂，pp. 112-121

４．発表年
2023年

１．発表者名
Qu, Q., Zhang, Y., and Kasahara, S.

２．発表標題
Auction game in intelligent reflecting surface aided secure communication

３．学会等名
第39回(2022年度)待ち行列シンポジウム「確率モデルとその応用」，早稲田大学本キャンパス小野記念講堂，pp. 29-30

４．発表年
2023年

１．発表者名
有薗舜，中畑裕，笠原正治

２．発表標題
時間変化するネットワークに対する二分決定グラフを用いた信頼性評価法

３．学会等名
2022年度OR学会関西支部 若手研究発表会

４．発表年
2022年

１．発表者名
Kasahara, S.

２．発表標題
A Matrix-Analytic Approach to Mining Process of Bitcoin Blockchain: How is the transaction-confirmation time affected by transaction arrival process?

３．学会等名
The International Teletraffic Congress ITC 34（招待講演）（国際学会）

４．発表年
2022年

１．発表者名
Hiraide Takumi、Kasahara Shoji

２．発表標題
A Mathematical Model of Blockchains Considering Dependencies of Fees, Confirmation Latency, and Security

３．学会等名
2022 International Conference on Emerging Technologies for Communications (ICETC2022)（国際学会）

４．発表年
2022年

１．発表者名
杉原健斗，原崇徳，笹部昌弘，笠原正治

２．発表標題
VNFの多様性・冗長性に基づく可用性と資源効率を考慮したサービスチェイニングとVNF配置方式

３．学会等名
電子情報通信学会技術研究報告（NS2022-167），pp. 1-6

４．発表年
2023年

１．発表者名
平出託海，笠原正治

２．発表標題
A mathematical model of user-miner interaction through confirmation latency and fees in Bitcoin-type blockchains

３．学会等名
第39回（2022年度）待ち行列シンポジウム「確率モデルとその応用」，早稲田大学本キャンパス小野記念講堂，pp. 112-121

４．発表年
2023年

１．発表者名
Qu, Q., Zhang, Y., and Kasahara, S.

２．発表標題
Auction game in intelligent reflecting surface aided secure communication

３．学会等名
第39回（2022年度）待ち行列シンポジウム「確率モデルとその応用」，早稲田大学本キャンパス小野記念講堂，pp. 29-30

４．発表年
2023年

１．発表者名
有薗舜，中畑裕，笠原正治

２．発表標題
時間変化するネットワークに対する二分決定グラフを用いた信頼性評価法

３．学会等名
2022年度OR学会関西支部 若手研究発表会

４．発表年
2022年

１．発表者名
Muhammad, R.F., and Kasahara, S.

２．発表標題
The Role of Trust and Personality in Social Networking Services' Information Dissemination

３．学会等名
IEICE 2nd Global Net Workshop（国際学会）

４．発表年
2022年

１．発表者名
Wiraatmaja, C., Zhang, Y., Sasabe, M., and Kasahara, S.

２．発表標題
Implementation of Blockchain Technology in the Internet of Things

３．学会等名
IEICE 2nd Global Net Workshop（国際学会）

４．発表年
2022年

１．発表者名
Osmani, S., Sasabe, M., and Kasahara, S.

２．発表標題
Support Vector Machine based Detection of Block Withholding Attacks in a Bitcoin Mining Pool

３．学会等名
IEICE 2nd Global Net Workshop（国際学会）

４．発表年
2022年

１．発表者名
Atuhurra, J., Hara, T., Zhang, Y., and Kasahara, S.

２．発表標題
Effect of Imbalanced Data on Binary Classification

３．学会等名
IEICE 2nd Global Net Workshop（国際学会）

４．発表年
2022年

１．発表者名
Qu, Q., Zhang, Y., and Kasahara, S.

２．発表標題
Research Overview --On Eavesdropping Region Characterization in Hybrid Communication Systems--

３．学会等名
IEICE 2nd Global Net Workshop（国際学会）

４．発表年
2022年

１．発表者名
森順平，川原純，湊真一，笠原正治

２．発表標題
DAGに対する幅とアルゴリズムに関する一考察

３．学会等名
情報処理学会 第84回全国大会，5K-05，pp. 1-229-1-230

４．発表年
2021年

１．発表者名
平出託海，笠原正治

２．発表標題
手数料・承認遅延・セキュリティの依存関係を考慮したブロック・チェーン数理モデルの検討

３．学会等名
第38回（2021年度）待ち行列シンポジウム「確率モデルとその応用」，pp. 166-167

４．発表年
2022年

１．発表者名
Qu, Q., Zhang, Y., and Kasahara, S.

２．発表標題
Analysis of Eavesdropping Region in Hybrid Wireless Communications Using Physical Layer Security

３．学会等名
第38回（2021年度）待ち行列シンポジウム「確率モデルとその応用」, pp. 91-100

４．発表年
2022年

１．発表者名
Atuhurra, J., Hara, T., Zhang, Y., and Kasahara, S.

２．発表標題
On Attack Pattern Classification in IoT Networks for Network Intrusion Detection Systems

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
2021年

１．発表者名
Matsunaga, T., Zhang, Y., Sasabe, M., and Kasahara, S.

２．発表標題
Reward and Penalty Mechanism in Proof-of-Stake Consensus Algorithm for Blockchain,

３．学会等名
2020 International Conference on Emerging Technologies for Communications (ICETC2020)（国際学会）

４．発表年
2020年

１．発表者名
源芳朗, 張元玉, 笹部昌弘, 笠原正治

２．発表標題
Reputation-Based Reward Distribution Mechanism for Blockchain-Based Scientific Paper Publishing Systems

３．学会等名
電子情報通信学会技術研究報告 (NS2020-171), pp. 287-292, 2021.3.5.

４．発表年
2020年

１．発表者名
Qu, Q., Zhang, Y., and Kasahara, S.

２．発表標題
Millimeter Wave vs. Microwave: Which Do Eavesdroppers Prefer?

３．学会等名
待ち行列シンポジウム「確率モデルとその応用」, pp. 42-50, オンライン開催, 2021.1.25.

４．発表年
2020年

１．発表者名
松永趨尭, 張元玉, 笹部昌弘, 笠原正治

２．発表標題
Proof-of-Stake型ブロック・チェーンの参加ノードへのインセンティブづけに関する一検討

３．学会等名
電子情報通信学会技術研究報告 (NS2020-86), pp. 62-67, 2020.11.27.

４．発表年
2020年

１．発表者名
馬場瑛義, 川原純, 笠原正治

２．発表標題
メニエルグラフと交差弦グラフを表すZDDの構築アルゴリズム

３．学会等名
情報処理学会研究報告 アルゴリズム (AL) , vol. 2020-AL-180, no. 5, pp. 1-6, 2020.11.25.

４．発表年
2020年

１．発表者名
Kasahara, S.

２．発表標題
Bitcoin Mining Mechanism -From a Queueing Theory Perspective-

３．学会等名
The International Teletraffic Congress (ITC 32) (招待講演) (国際学会)

４．発表年
2020年

１．発表者名
藤田 健太郎，張 元玉，笹部 昌弘，笠原 正治

２．発表標題
Block Withholding Attackが存在する場合のマイニングプール選択問題

３．学会等名
電子情報通信学会技術研究報告（NS2019-189），pp. 71-76，2020.3.5.

４．発表年
2020年

１．発表者名
豊 美玲，張 元玉，笹部 昌弘，笠原 正治

２．発表標題
Ethereumブロックチェーンを用いたIoT向け分散型属性ベース・アクセス 制御方式のコスト評価

３．学会等名
電子情報通信学会技術研究報告（NS2019-189），pp. 77-82，2020.3.5.

４．発表年
2020年

１．発表者名
山本 将成，笹部 昌弘，張 元玉，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
電子情報通信学会技術研究報告（NS2019-191），pp. 83-81，2020.3.5.

４．発表年
2020年

１．発表者名
中西 瑠海，張 元玉，笹部 昌弘，笠原 正治

２．発表標題
IOTAに基づいたIoTアクセス制御方式の設計と実装

３．学会等名
電子情報通信学会技術研究報告（NS2019-230），pp. 295-300，2020.3.6.

４．発表年
2020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
電子情報通信学会技術研究報告（CQ2019-88），pp. 1-6，2019.11.21.

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
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

３．学会等名
電子情報通信学会2019年ソサイエティ大会，講演論文集，B-11-10，2019.9.10.

４．発表年
2019年

１．発表者名
森 順平，川原 純，湊 真一

２．発表標題
次数制限付きハッセ図表現の情報理論的下限

３．学会等名
電子情報つ信学会技術研究報告（COMP2019-53），pp. 51-56，2020.3.

４．発表年
2020年

〔図書〕　計0件

〔産業財産権〕

〔その他〕
超スケーラブル汎用ブロック・チェーン技術に向けた情報学的研究
http://www-lsm.naist.jp/project/ultra-scalable_blockchain_technology/
超スケーラブル汎用ブロック・チェーン技術に向けた情報学的研究
http://www-lsm.naist.jp/blockchain-study/
超スケーラブル汎用ブロック・チェーン技術に向けた情報学的研究
http://www-lsm.naist.jp/blockchain-study

6．研究組織

| | 氏名<br>（ローマ字氏名）<br>（研究者番号） | 所属研究機関・部局・職<br>（機関番号） | 備考 |
|---|---|---|---|
| 研究分担者 | 笹部　昌弘<br>(Sasabe Masahiro)<br>(10379109) | 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<br>(14603) | |
| 研究分担者 | 川原　純<br>(Kawahara Jun)<br>(20572473) | 京都大学・情報学研究科・准教授<br>(14301) | |
| 研究分担者 | 原　崇徳<br>(Hara Takanori)<br>(70907881) | 奈良先端科学技術大学院大学・先端科学技術研究科・助教<br>(14603) | |
| 研究分担者 | 中畑　裕<br>(Nakahata Yu)<br>(50942067) | 奈良先端科学技術大学院大学・先端科学技術研究科・助教<br>(14603) | |
| 研究分担者 | 張　元玉<br>(Zhang Yuanyu)<br>(90804013) | 奈良先端科学技術大学院大学・先端科学技術研究科・助教<br>(14603) | |

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 |
|---|---|