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　 ６ 月 １３ 日現在

機関番号：１７１０２
研究種目：基盤研究(B)（一般）
研究期間：2018～2020
課題番号：１８Ｈ０３２４０

研究課題名（和文）暗号仮想通貨群のセキュリティとプライバシーに関する体系的理論評価

研究課題名（英文）Systematic Evaluation on Security and Privacy of Crypto-Virtual Currency

研究代表者
櫻井　幸一（SAKURAI, KOUICHI）

九州大学・システム情報科学研究院・教授

研究者番号：６０２６４０６６

交付決定額（研究期間全体）：（直接経費）　　13,500,000円

研究成果の概要（和文）：ビットコインをはじめとする暗号仮想通貨群では、暗号論的関数や公開鍵電子署名が利用されている。それら暗号アルゴリズム単体での安全性は、すでに学術的に研究評価されている。こしかし、通貨利用プロトコルの信頼性や応用サービスのプライバシー解析は、いまだに十分ではない。
本研究では、ビットコインやその亜種、ブロックチェーンなど暗号アルゴズムを利用した仮想通貨や契約サービスシステムの安全性を、学術的に評価した。また、匿名性と個人情報の関連結性も、分散計算プロトコルの解析に基づき、理論的にも解析した。さらに、基盤アルゴリズムやプトロコルの修正による、安全性や匿名性の強化も研究した。

研究成果の学術的意義や社会的意義
ビットコインや暗号仮想通貨は１０００種以上提案されている。利便性だけでなく、安全性や匿名性の強化を主張する方式も多い。しかし、多くは、提案・実装者による自己評価/ホワイトペーパーに留まっている。逆に、ビットコイン自体ですら、当初から危惧されていたハードフォーク問題が現実となり、分裂騒動が絶えない現状にある。これを背景に、新規提案よりも、既存提案の安全性や匿名性評価を、客観的に与えることが、社会的にも重要との認識に至った。安全性の解析は、学会レベルでも検討が始まっているが、徹底した議論ができている状況ではない。本研究は、この安全性評価へ学術的に貢献するものである。

研究成果の概要（英文）：Cryptographic functions and public key digital signatures are used in cryptographic virtual currencies including Bitcoin. The security of these cryptographic algorithms themself has already been well studied and evaluated academically. However, the reliability of currency utilization protocols and the privacy analysis of applied services are not sufficient yet. This study academically evaluated the security of virtual currencies and smart contract systems that use cryptographic algorithms such as Bitcoin, its variants, and blockchain. In addition, the relationship between anonymity and personal information was also theoretically analyzed based on the analysis of the distributed cryptographic protocol. We also investigated the enhancement of security and anonymity by modifying the basic algorithms and Protocols.

研究分野：サイバーセキュリティ

キーワード：暗号　仮想通貨　分散計算　プライバシー保護　ブロックチェーン　匿名通信　ハッシュ関数　分散データベース

様　式　Ｃ－１９、Ｆ－１９－１、Ｚ－１９（共通）

１．研究開始当初の背景

ビットコインは、実働・普及し、その応用サービスが注目されている。創始者 NAKAMOTO の原論文は短いが、オープンソースに至るまで、新しいアイデアや斬新な実装技法が隠されており、学術的にも賞賛できるほど、古典的計算機科学の課題に対するブレイクスルーを達成している。代表的には

[A]分散計算におけるビザンチン合意問題の解決[The Bitcoin Backbone Protocol: Analysis and Applications, Garay, Kiayias and Leonardos, Proc.EUROCRYPT-2015]

[B]分散データベースとしての CAP 定理の再考察の舞台[BigchainDB: A Scalable Blockchain Database, McConaghy, Marques, Muller, De Jonghe, McConaghy, cMullen, Henderson, SBellemare,Granzotto, 2016 ascribe GmbH,Germany]

[C]弱困難な暗号関数の計算難易度制御[Revisiting Difficulty Control for Blockchain Systems, Meshkov, Chepurnoy, and Jansenm, Proc. International Workshop on Cryptocurrencies and Blockchain Technology – CBT'17]

などが挙げられる。これらの課題は、分散計算と暗号理論や、また分散データベースとセキュリティ工学との境界領域という興味深い研究対象である。

ビットコインの寿命に関しては、ネットの解説などでも、投資の観点からは議論されている。ビットコインは、広く分散計算モデルの実現例の 1 つであるが、P2P ネットワーク上で、ノード数がユーザー数に対応するため、数万から百万個と、これまでにない巨大なネットワークを構成する。このため、実装の観点からユーザー数の限界解明は議論さている［"On the Necessity of a Prescribed Block Validity Consensus: Analyzing Bitcoin Unlimited Mining Protocol", R. Zhang and B.Preneel, CoNEXT'17: The 13th International Conference on emerging Networking EXperiments and Technologies]。

データの健全性確保には電子署名が利用され、プライバシー保護には匿名署名が活用される(e.g. 亜種コイン MORENO)。それまでの学術研究では、ユーザー数の増加に伴う署名長の増加は、漸近論で線形や指数オーダーなどが解析されてきた。しかし、 超多数のユーザーが利用する場合は、ユーザー数に依存しない、定数オーダー以下の時間と記憶容量が要求される。これまで、理論的な比較基準だった計算量の問題に、仮想通貨は、現実的な条件を課しており、この解決は、学術的にも意義ある課題である。

２．研究の目的

本研究は、暗号理論をはじめ計算機科学とデータベースやネットワークを含むセキュリティ工学の観点から、ビットコインや亜種暗号通貨の解析を行う。実働し多くの資産が投入されているビットコインとその亜種通貨の危殆寿命とプライバシー強度を、学術研究の立場から客観的に評価し、利用者にガイドラインを提供することを目的とする。

３．研究の方法

研究の遂行形態と実行計画：本研究では、研究代表者のグループが、すでに調査した仮想通貨群の解析を行い、安全性やプライバシーの強度を評価し、脆弱性解析、解析成果を意識した改良と再評価、類似関連研究との比較評価や最新研究成果の取り込みを行なった。特に、安全性の議論での暗号論的な仮定の明瞭化や、実装における上限、高速化や取り込めるデータタイズの限界の定量的解析を行なった。

研究期間は、当初は4年でなく3年間とした。理由は、この分野の社会状況の変化に適応するためであった。しかし、コロナの影響での研究遂行障害もあり、結果的には半年間の延長で、3年半の研究期間となった。

研究協力体制は、過去から現在までに共同研究と共著論文のある3名の分担者（会津大の蘇、長崎県立大の穴田、そして九大のフォン）、専門性の観点からそれぞれがサブテーマを主導した。また、一部のテーマは、代表者の研究室の学生らも取り組み、卒業研究で成果を出し、外部発表を行った。また、仮想通貨の匿名性と追跡性に関しては、実質的な外部研究者の才所（IT 企画）との共同研究を遂行し、一連の成果を外部発表した。

4. 研究成果

4.1 当初計画していの3つのサブテーマに対して、それらの成果を外部発表した。

(S1)ハッシュ関数の計算困難性制御 [穴田(主担当)＆櫻井・蘇(副担当)]

ブロックチェーン技術における処理の工程の一つに，提示された計算困難問題のインスタンスの解を探索し，発見した証拠をプルーフ・オブ・ワークとして示す工程がある．探索はマイナー(採掘者)により競争的に行われ，探索時間は問題の困難さに依存する．プルーフ・オブ・ワークの工程のあるブロックチェーン技術では，探索時間を調節する仕組みがあることが多く，困難度制御(difficulty control)と呼ばれている．本研究では、ビットコインや亜種における、ハッシュ計算困難さの制御アリゴリズムの解析を行なった。確率論を駆使した理論解析を基盤とし、さらに、具体的な関数に対して、計算機実験による解析評価も行なった。

暗号ハッシュ関数を利用した仮想通貨採掘の時間分散に対する計算機実験評価[池辺・櫻井 IEICE/ISEC2021]: 仮想通貨は取引を行う際にマイニングという、計算困難な問題の解の探索を行っている。探索の性質上、マイニングにかかる時間にはブレが生じてしまう。これは仮想通貨ゲームの観点から好ましくない。この研究では、マイニングにかかる時間の分散を小さくするため、穴田らの先行研究で提案された複数連結マイニングを実装し、性能評価を行った。その結果、理論解析値とは多少異なる結果となったが、小分散化の効果が実験的にも確認できた。

グラフ・クリーク探索問題を利用した仮想通貨採掘時間の分散解析[池辺・櫻井 FIT2021: ビットコインのマイニングはナンスの探索によって行われるが、その探索時間の期待値は事前に設定した難易度によって決められている.期待値よりも非常に早い時間でマイニングを完了させることが出来てしまうと、攻撃者がブロックの分岐などを引き起こす恐れがある。このため、マイニングにかかる時間の分散は小さいことが望まれる。しかしビットコインでは、その特性上マイニングに要する時間の分散が大きくなるという問題が内在する。 本研究では、穴田や櫻井らの先行研究で提案されていたハッシュ関数の連結による小分散化とクリーク探索を利用したマイニングアルゴリズムによる小分散化の二つの手法を組み合わせることで、さらに小分散化できることを実現に検証した。

(S2) 匿名性と関連結性 [穴田(主担当)＆蘇・櫻井(副担当)]

ビットコインは、利用者の匿名性を実現しているが、トランザクション次第では、利用者の情報が漏れることが知られている。より強力な匿名性を実現する MORENO では、Rivest らが開発した環(ring)署名 [Rivest , Shamir, and Tauman, “How to Leak a Secret,” Advances in CryptologyーASIACRYPT 2001]を導入している。この MORENO の欠陥も最近指摘され[ESORICS2017]、さらなる改良 MORENO2.0 の開発も行われている。本研究でも、ビットコイン亜種に対する、同様の解析を行い、プライバシー強度を評価した。必要に応じて、匿名化暗号技術の導入と強化による改善方式の方向性も研究した。

暗号資産の封印・償還における利用者の匿名性および特定・追跡性の考察 [才所・辻井・櫻井, IEICE/SCIS2021]: 暗号資産を台帳に登録する情報内容により、資産移転記録方式と資産残高記録方式の 2 種に分類し、主要な暗号資産 Bitcoin、MONERO、Zcash を対象に、台帳に登録・公開される封印情報・償還情報に関する利用者の匿名性と特定・追跡性の現状を調査した。利用者の匿名性に関しては、ゼロ知識証明を利用している Zcash が台帳に登録する情報の中に利用者識別情報を露出させることなく封印・償還を実現しており、匿名性が高いといえる。利用者の特定・追跡性に関しては、MONERO では tracking key/鍵イメージ、Zcash では Incoming Viewing Key を利用者が提供することにより、台帳上の暗号資産/利用者識別情報と利用者の対応を特定可能である。しかし、未だ基本的な機能のみが実装されている状況で、利用者の特定・追跡性に関する具体的要求の明確化が課題であることを指摘した。

ビットコイン利用者の特定・追跡の仕組みに関する考察[才所・辻井・櫻井, IEICE/ICSS2021]
暗号資産の強い匿名性によるマネーロンダリングや不正・不法な取引の決済への利用が急増

しつつあり、暗号資産の悪用を防ぐ対策が求められている。各国政府は暗号資産関連事業者に対し確実な KYC（本人確認）を実施する等、法制度やガイドラインにより規制を強化している。しかし，多くの暗号資産は事業者を通さず利用者間での資産移転が可能なため、このような対策の効果は限定的であり、暗号資産の悪用を防ぐには、暗号資産システム側で利用者の特定・追跡のための仕組みを組み込む必要がある．本論文では、ビットコインシステムを対象に、P2PKH の資産移転方式に限定しているが、利用者であるトランザクション作成者の特定・追跡の仕組みの実現方式を複数提案し、その実現可能性、実現へのアプローチ案を与えた。今回の実現方式案は，資産移転記録ベースの多くの暗号資産システム（TCAMS）へ適用可能と想定されるが，それぞれの暗号資産システムごとに別途検討は必要となる。暗号資産システムへの利用者の特定・追跡の仕組みの組み込みについての検討は、未だこれからの状況にあることに注意する。インターネット社会の安心・安全な暗号資産システム、さらには各国での検討が活発になってきた CBDC（法定デジタル通貨）の検討においても。利用者の匿名性と特定・追跡の両立は，今後も多くの研究・開発が展開される重要な課題であることを指摘した。

(S4) 分散データベースとしてのブロックチェーン[Feng（主担当）&櫻井（副担当）]
ブロックチェーンは、仮想通貨としての応用だけでなく、分散台帳としての機能を切り出しての活用が注目され、ゼロ知識証明も応用されている[“ALHGORAND, a secure and efficient public legder”, J.Chen and S.Micali(MIT), arXiv &IACR-eprint 2017]。また分散台帳は、分散データベースの一種とみなせるが、ここには有名な Brewer(2000 年)の CAP(Brewer)定理[一貫性・可用性・分断耐性の 3 つを同時に満足するシステムは存在しない]が浮上する。イサリウムやビットコイン亜種の実装には、3 つの基本 CAP 性質のどれかを犠牲にするか、あるいは、どこかに比重を置いた設計が要求される。本研究では、代表的な仮想通貨の実装がどうなっているのか、CAP 定理を切り口に、解析分類を試みた。さらに、仮想通貨や応用サービスの要求を参照しながら、3 つの条件のどれを緩めて実装すべきか、強い CAP 定理[Vogels, Eventually Consistent, Comm. ACM Vol.52 (1), Jan. 2009] も参考に研究した。

ブロックチェーンプラットフォームと汎用トランザクション管理システム[フォン・櫻井 IPSJ/CSS 2020] ブロックチェーン技術は，大きなアプリケーションでも適用できることは既に分かっており，その産業的価値が確認されつつある。 ブロックチェーンはトランザクション管理システムに進化しているため，多くの企業や政府機関は，企業グレードのデータベースを置き換える、または補完するためにブロックチェーンを応用・開発している。 本研究では，ブロックチェーン技術とデータベース技術との融合の現状からブロックチェーンデータベースシステムの開発例および業者の動きまでを調査した。

4.2 国際連携・共同研究・国際会議

Sabyasachi Dutta は、NICT 国際共同研究招聘基金の支援を受けて、以前から JST 国際共同研究でも交流実績のあるインド統計研究所から1年間[2018-2019]のポスドクとして招聘できた。短期間であったが、分散暗号に関する本プロジェクトのテーマに興味を示し、国際会議や国内シンポジウムに本研究成果を発表した。（その後、カナダ・カリガリー大学のポスドクに移籍し、現在に至る。） Hawen Tan は、韓国で学位取得後、九大・サイバーセキュリティセンター・日印 Sicorp プロジェクト支援の研究員として1年間[2021-2022] 在外/online ではあったが、ブロックチェーンの研究に貢献し、修士学生らとの本研究に関する共同研究成果を発表した。（2022 年 4 月以降は、本国中国の大学の研究職に予定している。）

ACM AsiaCCS2022: 研究代表者は、この 5 月に開催沙汰 AsiaCCS2022(長崎・出島メッセ)の誘致から開催準備までを、4年かけて行なった。会議自体も、コロナ対策を意識して、会議発のハイブリッド形式となった。貴重講演の1つでは、Ta Rabin(元 IBM 研究所・現在はペンシルバニア大)によるビットコインにおける分散暗号認証モデルの改良”New Multiparty Computational Model: From Nakamoto to YOSO”が発表された。またワークショップの1つ ACM International Symposium on Blockchain and Secure Critical Infrastructure は4回目を迎えての併設開催(完全 virtual)となった。さらに本会議でも、ブロックチェーンに特化したセッションが設けられ、最先端の研究発表が行われた。ポスターセッションも、対面と virtual の混合形式が試みられ、ブロックチェーンや分散暗号系の発表も行われ、本研究分野の活性化と国

際化に貢献できたと評価している。

ACNS2021: 研究分担者の蘇は、第19回 International Conference on Applied Cryptography and Network Security の実行代表を務めた。当初は鎌倉での開催予定であったが、コロナのため、完全 online/virtual となった。ここでもデジタル ID やプライバシー保護型認証に関する基調講演が行われ、デジタル通貨に特化したセッションも設けられた。またワークショップの1つ International Workshop on Application Intelligence and Blockchain Security(AIBlock)も、蘇が主導し、4回目の併設開催となり、代表者の櫻井も、本研究の一環として、プログラム委員の立場で参画・協力した。

IEEE ICBC 2020: 2018 年ソウルから始まった IEEE International Conference on Blockchain and Cryptocurrency に日本からプロググラム委員に参画しているのは、代表の櫻井のみである（今回 2020 年には、もう一人の日本人が加わったが、所属はシンガポール国研 A-star 所属）。IEEE Blockchain は、2018 年より計算機分科会主催で始まり、数多くの投稿が集まり、大成功し、発展している、この 2020 年 online 会議の委員長を櫻井が、分担者の蘇がプログラム長をつとめ、本研究分野の国際活性化に貢献した。

4.3 現状と今後の課題

ブロックェーンの分野では、計画段階では予定していなかった技術が現在は注視されている、その1つが自己主権型認証であり、もう1つが非代価トークン（Non-Fungible Token, NFT）である。前者に関しては、共同研究者の才所らと調査研究を始めている[自己主権型アイデンティティ情報管理システム(uPort、Sovrin)考察, IEICE ソサイエティ大会 2021]。 後者に関しては、代表者が 10 年前に研究していた電子プロビナンス（ただし、当時は集中管理型）の再訪として、研究室での新しいテーマとして、また本研究の発展課題として取り組み始めたところである。

最新の現状としては、投資対象にもなっているビットコインに代表される仮想通貨（暗号資産）に対して、中央銀行が発行する法定通貨建てであるでデジタル通貨(Central Bank Digital Currency, CBCD)の実用化が進んでいる。ビットコインは広くは分散システムが、非中央集権型あるいは分権型システムと呼ぶべきともいえる。これは、公開鍵認証基盤 PKI が信頼できるセンターに基盤をおく中央集権型とは正反対である。PKI 以前の PGP(Pretty Good Privacy)という暗号化ソフトでの利用者登録は、友達の紹介による信頼の輪を広げるもので、中央管理者が存在しない民主型であった。ビットコインの基盤も、ある意味では PKI 以前の PGP 民主型基盤に戻ったとも言える。

こうした変化は、分散・分権基盤から再び中央管理基盤に戻る CBCD を手本に、新しいデジタル商取引を生み出す好機会であると同時に、新たなせキュリティとプライバシーの課題も危惧されており、学術の観点からの研究が、より一層に期待される。

//以上

５．主な発表論文等

〔雑誌論文〕　計12件（うち査読付論文　12件／うち国際共著　12件／うちオープンアクセス　3件）

１．著者名 Wang Weizheng、Huang Huakun、Zhang Lejun、Su Chunhua	４．巻 14
２．論文標題 Secure and efficient mutual authentication protocol for smart grid under blockchain	５．発行年 2020年
３．雑誌名 Peer-to-Peer Networking and Applications	６．最初と最後の頁 2681～2693
掲載論文のDOI（デジタルオブジェクト識別子） 10.1007/s12083-020-01020-2	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 該当する

１．著者名 Ma Limao、Kaneko Kosuke、Sharma Subodh、Sakurai Kouichi	４．巻 xxx
２．論文標題 Reliable Decentralized Oracle with Mechanisms for Verification and Disputation	５．発行年 2019年
３．雑誌名 CANDAR Workshops 2019	６．最初と最後の頁 346-352
掲載論文のDOI（デジタルオブジェクト識別子） 10.1109/CANDARW.2019.00067	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 該当する

１．著者名 Xu Guangquan、Guo Bingjiang、Su Chunhua、Zheng Xi、Liang Kaitai、Wong Duncan S.、Wang Hao	４．巻 88
２．論文標題 Am I eclipsed? A smart detector of eclipse attacks for Ethereum	５．発行年 2020年
３．雑誌名 Computers & Security	６．最初と最後の頁 101604～101604
掲載論文のDOI（デジタルオブジェクト識別子） 10.1016/j.cose.2019.101604	査読の有無 有
オープンアクセス 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 該当する

１．著者名 Lu Zhou, Chunpeng Ge, and Chunhua Su	４．巻 63
２．論文標題 A privacy preserving two-factor authentication protocol for the Bitcoin SPV nodes	５．発行年 2020年
３．雑誌名 Science China Information Sciences volume	６．最初と最後の頁 x-x
掲載論文のDOI（デジタルオブジェクト識別子） 10.1007/s11432-019-9922-x	査読の有無 有
オープンアクセス 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 該当する

1．著者名 Wang Wei、Song Jingjing、Xu Guangquan、Li Yidong、Wang Hao、Su Chunhua	4．巻 x
2．論文標題 ContractWard: Automated Vulnerability Detection Models for Ethereum Smart Contracts	5．発行年 2020年
3．雑誌名 IEEE Transactions on Network Science and Engineering (Early Access)	6．最初と最後の頁 1~1
掲載論文のDOI（デジタルオブジェクト識別子） 10.1109/TNSE.2020.2968505	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 該当する

1．著者名 Ma Limao、Kaneko Kosuke、Sharma Subodh、Sakurai Kouichi	4．巻 x
2．論文標題 Reliable Decentralized Oracle with Mechanisms for Verification and Disputation	5．発行年 2019年
3．雑誌名 019 Seventh International Symposium on Computing and Networking Workshops (CANDARW), Nagasaki, Japan, 2019	6．最初と最後の頁 346-352
掲載論文のDOI（デジタルオブジェクト識別子） 10.1109/CANDARW.2019.00067	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 該当する

1．著者名 Zhao Bo、Fang Liming、Zhang Hanyi、Ge Chunpeng、Meng Weizhi、Liu Liang、Su Chunhua	4．巻 19
2．論文標題 Y-DWMS: A Digital Watermark Management System Based on Smart Contracts	5．発行年 2019年
3．雑誌名 Sensors	6．最初と最後の頁 3091～3091
掲載論文のDOI（デジタルオブジェクト識別子） 10.3390/s19143091	査読の有無 有
オープンアクセス 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 該当する

1．著者名 Anada Hiroaki、Yasuda Takanori、Kawamoto Junpei、Weng Jian、Sakurai Kouichi	4．巻 45
2．論文標題 RSA public keys with inside structure: Proofs of key generation and identities for web-of-trust	5．発行年 2019年
3．雑誌名 Journal of Information Security and Applications	6．最初と最後の頁 10～19
掲載論文のDOI（デジタルオブジェクト識別子） 10.1016/j.jisa.2018.12.006	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 該当する

1．著者名 Shota Johjima、Kosuke Kaneko、Sharma Subodh、Kouichi Sakurai	4．巻 926
2．論文標題 Simulation of Secure Volunteer Computing by Using Blockchain	5．発行年 2019年
3．雑誌名 AINA 2019, Advances in Intelligent Systems and Computing	6．最初と最後の頁 883～894
掲載論文のDOI（デジタルオブジェクト識別子） 10.1007/978-3-030-15032-7_74	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 該当する

1．著者名 Anada Hiroaki、Matsushima Tomohiro、Su Chunhua、Meng Weizhi、Kawamoto Junpei、Bag Samiran、Sakurai Kouichi	4．巻 11449
2．論文標題 Analysis of Variance of Graph-Clique Mining for Scalable Proof of Work	5．発行年 2019年
3．雑誌名 Information Security and Cryptology - 14th International Conference, Inscrypt 2018, Revised Selected Papers. Lecture Notes in Computer Science	6．最初と最後の頁 101～114
掲載論文のDOI（デジタルオブジェクト識別子） 10.1007/978-3-030-14234-6_6	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 該当する

1．著者名 Nishida Yuki、Kaneko Kosuke、Sharma Subodh、Sakurai Kouichi	4．巻 1
2．論文標題 Suppressing Chain Size of Blockchain-Based Information Sharing for Swarm Robotic Systems	5．発行年 2018年
3．雑誌名 Sixth International Symposium on Computing and Networking, CANDAR Workshops 2018,	6．最初と最後の頁 524-528
掲載論文のDOI（デジタルオブジェクト識別子） 10.1109/CANDARW.2018.00102	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 該当する

1．著者名 Talukder Asoke K、Chaitanya Manish、Arnold David、Sakurai Kouichi	4．巻 1
2．論文標題 Proof of Disease: A Blockchain Consensus Protocol for Accurate Medical Decisions and Reducing the Disease Burden	5．発行年 2018年
3．雑誌名 IEEE SmartWorld/SCALCOM/UIC/ATC/CBDCom/IOP/SCI 2018,	6．最初と最後の頁 257-262
掲載論文のDOI（デジタルオブジェクト識別子） 10.1109/SmartWorld.2018.00079	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 該当する

〔学会発表〕　計15件（うち招待講演　2件／うち国際学会　3件）

1．発表者名
○才所敏明 ， 辻井重男 ， 櫻井幸一

2．発表標題
ビットコイン利用者の特定・追跡の仕組みに関する考察

3．学会等名
電子情報通信学会技術研究報告 ICSS

4．発表年
2021年

1．発表者名
○池辺 慶，櫻井 幸一

2．発表標題
暗号ハッシュ関数を利用した仮想通貨採掘の時間分散に対する計算機実験評価

3．学会等名
電子情報通信学会技術研究報告 ISEC

4．発表年
2021年

1．発表者名
○池辺 慶，櫻井 幸一

2．発表標題
グラフクリーク探索問題を利用した仮想通貨採掘時間の分散解析

3．学会等名
電子情報通信学会　2021年 情報科学技術フォーラム(FIT)

4．発表年
2021年

1．発表者名
○Hiroaki Anada, Kouichi Sakurai

2．発表標題
Exponential Distribution of Hash-Mining Time and its Serial/Parallel Variations for Smaller Variance

3．学会等名
The 2021 IEEE Conference on Dependable and Secure Computing, Poster（国際学会）

4．発表年
2021年

１．発表者名
○フォン　ヤオカイ、櫻井　幸一

２．発表標題
ブロックチェーンプラットフォームと汎用トランザクション管理システム

３．学会等名
IPSJ/コンピュータセキュリティシンポジウム 2020

４．発表年
2020年

１．発表者名
○穴田 啓晃，櫻井 幸一

２．発表標題
ハッシュ関数に基づく計算問題に対するマイニング時間の小分散化~直列連結及び並列連結~

３．学会等名
電子情報通信学会技術研究報告 ISEC

４．発表年
2020年

１．発表者名
○穴田 啓晃，櫻井 幸一

２．発表標題
ハッシュマイニングにおけるブロック到着時間の小分散化

３．学会等名
2020年暗号と情報セキュリティシンポジウム

４．発表年
2020年

１．発表者名
○才所敏明，辻井重男，櫻井幸一

２．発表標題
DAG技術ベースの暗号資産の匿名性に関する考察

３．学会等名
2020年暗号と情報セキュリティシンポジウム

４．発表年
2020年

１．発表者名
○才所 敏明， 辻井 重男，櫻井 幸一

２．発表標題
匿名暗号資産（Monero/Zcash/Grin）ブロックチェーンの匿名性に関する考察

３．学会等名
コンピュータセキュリティシンポジウム 2019

４．発表年
2019年

１．発表者名
○穴田 啓晃

２．発表標題
第9回バル=イラン大学冬季暗号学スクール参加報告

３．学会等名
電子情報通信学会 暗号と情報セキュリティ 研究会　信学技報，vol．119，no．140，ISEC2019-55，pp．357-361，2019年7月．

４．発表年
2019年

１．発表者名
Kouichi SAKURAI

２．発表標題
E-voting scheme after Blockchain: A challenge of achieving "Receipt-freeness"

３．学会等名
The 2nd International Workshop on Blockchain and its Applications (Blockchain 2019) 広州（招待講演）（国際学会）

４．発表年
2019年

１．発表者名
Kouichi SAKURAI

２．発表標題
Security of Electronic Voting Schemes after Blockchain

３．学会等名
13th International Conference on Network and System Security (NSS2019) 札幌（招待講演）（国際学会）

４．発表年
2019年

１．発表者名
馬 立茂 , 金子 晃介 , 櫻井幸一

２．発表標題
スマートコントラクトにおける信頼性ある分散型オラクル手法の提案

３．学会等名
火の国シンポジウム2019

４．発表年
2019年

１．発表者名
才所敏明 辻井重男,櫻井幸一

２．発表標題
仮想通貨の匿名性の現状と課題

３．学会等名
暗号と情報セキュリティシンポジウム（SCIS）

４．発表年
2019年

１．発表者名
才所敏明 辻井重男,櫻井幸一

２．発表標題
暗号仮想通貨における匿名化技術の現状と展望

３．学会等名
IPSJ 全国大会（福岡大学）

４．発表年
2019年

〔図書〕　計2件

１．著者名	４．発行年
Satyanarayana V Lokam , Sushmita Ruj, Kouichi Sakurai	2019年
２．出版社	５．総ページ数
ACM Special Interest Group on Security, Audit and Control	25
３．書名	
BCC '19: Proceedings of the Third ACM Workshop on Blockchains, Cryptocurrencies and Contracts	

1．著者名	4．発行年
Satya LOKAM, Sushmita RUJ, Kouichi SAKURAI	2018年
2．出版社	5．総ページ数
ACM	63
3．書名	
Proceedings of the 2nd ACM Workshop on Blockchains, Cryptocurrencies, and Contracts	

〔産業財産権〕

〔その他〕

九州大学-研究者情報: [櫻井 幸一
https://hyoka.ofc.kyushu-u.ac.jp/search/details/K000220
九州大学-研究者情報: 馮 尭鍇（フォン ヤオカイ、Feng Yaokai）
https://hyoka.ofc.kyushu-u.ac.jp/search/details/K002276/index.html
九州大学研究者情報
http://hyoka.ofc.kyushu-u.ac.jp/search/details/K000220/

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
研究分担者	ＳＵ　Ｃｈｕｎｈｕａ (Su Chunhua) (40716966)	会津大学・コンピュータ理工学部・上級准教授 (21602)	
研究分担者	穴田　啓晃 (Anada Hiroaki) (40727202)	長崎県立大学・情報システム学部・教授 (27301)	2022年4月より青森大学・教授へ転籍。
研究分担者	馮　尭楷 (Feng Yaokai) (60363389)	九州大学・システム情報科学研究院・助教 (17102)	

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