

令和 7 年 6 月 20 日現在

機関番号：25403

研究種目：基盤研究(C)（一般）

研究期間：2021～2024

課題番号：21K11891

研究課題名（和文）ブロックチェーンでファンジビリティとセキュリティを両立するための自己防衛方式

研究課題名（英文）Self-defense mechanisms for preventing transaction commitment without recipient authorization on blockchains

研究代表者

上土井 陽子（Kamidoi, Yoko）

広島市立大学・情報科学研究科・准教授

研究者番号：80264935

交付決定額（研究期間全体）：（直接経費） 3,100,000円

研究成果の概要（和文）：ブロックチェーンでは通貨の等価交換性を意味するファンジビリティの維持が重要であるが、犯罪に関連した資金の流入も指摘されている。本研究ではブロックチェーンの公開情報の悪用による利用者の犯罪への巻き込みや見知らぬ貸付けの可能性を排除するため、(1)ファンジビリティを維持したままで、利用者が公開情報の無断利用を選択的に排除できる自己防衛方式を新たに提案し、(2)既存のBitcoin、Ethereumブロックチェーンに導入するための実現方法を提案し、(3)導入による取引作成の計算コストのオーバーヘッドがBitcoinでは概ね2倍程度、Ethereumでは約5%増となり、合理的であることを確認した。

研究成果の学術的意義や社会的意義

ブロックチェーンにて安定した通貨を提供したり、公共のサービスを提供するには、連結可能性、追跡可能性を防ぎ、ファンジビリティを維持する必要がある。一方で、ファンジビリティを維持することは、マネーロンダリングなどの犯罪に関連した資金が暗号資産に流入する可能性を高めてしまう。よって、犯罪に関連した資金がブロックチェーンに関与しないという状況にすることは難しい。

本研究ではプライバシー漏洩が起きてしまった場合でもユーザーが承認していない取引との関連を分散台帳に記録されることを自身が防ぐ手段を提供した。本研究成果により、現在よりも広い公共サービスを提供できる分野でのブロックチェーンの活用が期待できる。

研究成果の概要（英文）：In recent years, blockchain is utilized practically as a distributed secure digital ledger of transactions. Blockchain is regarded as one of the most important next generation infrastructure technologies of the financial industry, as well as artificial intelligence and big data. Although many researchers have studied for various types of issues on blockchain, there always exist security and privacy concerns.

In this research, we point out a new concern for abusing the publicity of blockchain and also show the possibility of suspicions aroused by the concern. Then we propose two selective mechanisms for self-protecting against the approach from crimes or computer viruses on blockchains such as Bitcoin and Ethereum, whether the disclosure of user's privacy occurs or not. We introduced and implemented two mechanisms on open-source software for Bitcoin developers and Ethereum developers. The experimental results demonstrated that the overhead of introducing the mechanisms are reasonable.

研究分野：情報工学

キーワード：ブロックチェーン 受領者未承認取引 ファンジビリティ 暗号通貨 Bitcoin Ethereum

1. 研究開始当初の背景

ブロックチェーン以前の電子通貨ではデジタル署名を用いて授受することで支払い者の認証は可能であったが、複製の作成が容易な電子通貨を支払い者が2回以上用いる二重支払い問題が解決できないため、信頼できる第三者（銀行、カード会社等）の仲介が必要だった。しかし、Satoshi Nakamotoによって、上記の二重支払い問題を第三者機関や中央集権的な組織の介入なしに解決する画期的な方法であるブロックチェーンが提案された。ブロックチェーンは分散台帳とみなせる巨大な分散データベースの一貫性を Peer-to-Peer (P2P) ネットワーク上のノード間で動作する合意アルゴリズムを使って維持する技術である。そこで用いられる合意アルゴリズムは Proof-of-Work という暗号技術を利用した膨大な計算量を必要とする処理である。

ブロックチェーン上で管理される電子通貨は暗号技術に支えられているため暗号通貨と呼ばれる。代表的な暗号通貨として Bitcoin、Ethereum 等があり、2020年の時点で約3700億ドルの時価総額となっている。また、Bitcoin、Ethereum ではそれぞれのブロックチェーンのプロトコルとしてオープンソースソフトウェア BitCore、GoEthereum を利用している。それぞれのソースコードは開発者を支援する Web サービス GitHub にて公開されており、透明性が高い。

一方、ブロックチェーンに関しては、P2P ネットワークの51%問題のような規模に関する課題やプライバシー保護、セキュリティに関する課題も指摘されている。その中でも、最重要な課題はファンジビリティの維持である。ファンジビリティとは取引内容や移転経路によらず同額であれば交換可能という通貨において維持すべき性質である。取引が全て公開されている暗号通貨では特に維持が難しい性質でもあるが、ブロックチェーンの安定した普及やプライバシー保護の観点から、ミキシングサービスなど積極的に対策が施されファンジビリティの課題は解決されつつある。しかし、ファンジビリティを維持することで、犯罪を検出するために必要な追跡可能性が失われることとなり、マネーロンダリングなどの犯罪に関連した資金がブロックチェーン上で取引されていることが確認されている。よって、犯罪資金の流入の規制強化と共に、犯罪資金に関連する取引から健全な利用者を守るセキュリティ機能のブロックチェーンへの導入が新たな課題として出現している。

2. 研究の目的

本研究ではブロックチェーンにおいてファンジビリティを維持したままで、利用者が公開情報の無断悪用を選択的に排除できる自己防衛のセキュリティ方式を提案、実現、標準化することを目的とする。具体的には、最も一般的な暗号通貨である Bitcoin のブロックチェーン上で提案方式を実現し、標準化に向けた課題を整理するため、**【課題1】提案方式の BitCore への組み込みの実現と安全性と計算処理コストの性能解析**を行い、さらに、スマートコントラクト等へも対応可能な別の一般的な暗号通貨である Ethereum のブロックチェーンにおける**【課題2】提案方式の GoEthereum への組み込みの実現と性能解析**を行う。最後に、Bitcoin、Ethereum それぞれのオープンソースソフトウェアへの提案方式の組み込みを標準化プロセスに提案し、標準化への審査を受けるために**【課題3】標準化プロセスへの提案と実用化に向けた調整**を行う。以上により、受領者が選択的に利便性を考慮しながら、分散台帳の自己の記録を防衛することが可能となり、ブロックチェーンの健全性を一層高めることができる。

3. 研究の方法

本研究では研究目的を達成するため、以下の3つの課題に分けて考察した。

【課題1】受領者のための選択的自己防衛方式の提案と BitCore への組み込みの実現と安全性と計算処理コストの性能解析

本課題では我々の準備的研究で開発した取引作成プロトコルとアドレス作成手続きを複数の安全性レベルを持つプロトコル、手続きに拡張し、実際の Bitcoin 公式クライアントソフトウェアであり、そのソースコードが公開されている BitCore に組み込む。このとき、Bitcoin での従来の記述と親和性の高い提案取引の記述方法を提案する。また、受領者の認証を組み込む場合に

は公開鍵を受領時にも記載せねばならず、入金された暗号資産の安全性が低下する可能性がある。よって、安全性の向上と取引記述量の増加や検証処理コストの増加を勘案した複数の選択肢を実現し、提案方式の実現の安全性とコストのトレードオフの関係を理論的・実験的に解析する。

【課題2】提案方式の GoEthereum への組み込みの実現と性能解析

課題1の Bitcoin での提案方式の実現を Ethereum 公式クライアントソフトウェア GoEthereum に移植し、Bitcoin とはアドレス管理方法が大きく異なる Ethereum ブロックチェーンでの提案方式の実現の詳細化を行い、Ethereum での提案方式の実現の安全性とコストのトレードオフの関係を理論的・実験的に解析する。

【課題3】標準化プロセスへの提案と実用化に向けた調整

課題1、2での提案方式の実現における解析結果より提案方式の実現の中で安全性とコストのバランスが優れた実現を Bitcoin の改善と提案の標準化プロセスである BIP(Bitcoin Improvement Proposal)と EIP(Ethereum Improvement Proposal)に提案し、安全性の課題を指摘すると共に標準化への審査を受け、実用化に向け調整する。また、本研究課題の成果を国内研究会、国際会議などで発表し、学术论文としてまとめるとともに、特許としても出願する。

4. 研究成果

本研究の研究成果を各課題に分けて示す。

【課題1】に関する研究成果：

交付決定前の期間に課題1の一部を事前に実施し、結果をまとめ2021年1月に論文投稿を行った。結果は2021年2月に論文(Yoko Kamidoi, Ryouzuke Yamauchi, and Shin'ichi Wakabayashi, "A protocol for preventing transaction commitment without recipient's authorization on blockchain and its implementation," IEEE Access, Vol. 9, pp.24390-24405)として掲載された。事前研究では図1に示す提案方式を Bitcoin の基盤ソフトウェアである Bitcoin Core に組み込むことを目的に具体的に2つの安全強度の異なる新しいアドレス型をもった選択的方式に拡張し、安全性を理論的に証明し、Bitcoin ソフトウェア開発用ライブラリ libbitcoin [3]を用いて取引作成手続き、および、通貨管理手続きを実現した。シミュレーション実験の結果、提案方式の導入による取引作成のオーバーヘッドが実用的な範囲であることがわかった。また、交付決定前の期間に研究に関連する特許出願(2019年3月14日出願：発明の名称「ブロックチェーン取引作成プロトコル、及びブロックチェーンアドレス作成方法」、特願2019-045801、特許権者：公立大学法人広島市立大学、発明者：上土井陽子、若林真一、山内涼介)を行っていたが、2021年8月に特許登録(特許第6934679号)となった。

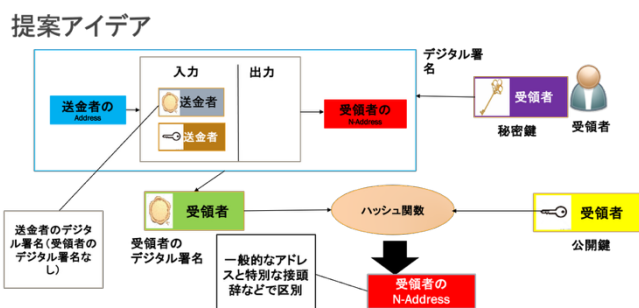


図1 Bitcoinに関する提案方式概要

さらに、ユーザが取引作成に利用する Wallet と呼ばれるソフトウェアに提案方式を組み込むことを考察し、libbitcoin を用いて取引作成手続きをシミュレーション実験環境に実現し、送金者、受領者のデジタル署名などを行う取引作成の計算時間を計測した。実験の結果、取引作成の実行時間は従来手続きの実行時間と比べ118%の増加となり、約2.2倍となった。また、受領した暗号通貨を確認し Wallet に記録するまでの実行時間は従来と比べ12%増加となった。

最後に、Bitcoin Wallet に関する提案方式での送金者と受領者の情報交換方法を送金者と受領者間の信頼関係に応じて選択可能とするための機能追加の方針を決定した。

[課題2]に関する研究成果：

Ethereum ブロックチェーンへの提案方式の組み込みに関し調査した結果、Ethereum ブロックチェーンでは残高管理のモデル（アカウントモデル）がBitcoin ブロックチェーンでの残高管理のモデルであるUnspent Transaction Output (UTXO)モデルと大きく異なるため、課題1での提案方式の導入が難しいことがわかった。そのため、図2に示すEthereumに関する新しい選択的自己防衛方式の概略を決定した。

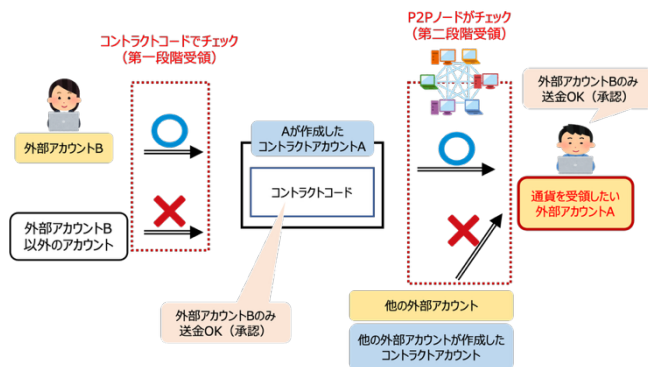


図2 Ethereumに関する提案方式概要

具体的には、Ethereumでの残高管理モデルであるアカウントモデルではブロックチェーンに各アカウントの状態も記録されるため、アカウントに自己防衛の仕組みを組み込み、Ethereum Virtual Machine (EVM) と呼ばれる仮想マシンにてプログラムを実行させる新しい選択的自己防衛方式を提案した。提案方式ではスマートコントラクトと呼ばれるプログラム記載可能なアカウントを活用し、受領者が認めた送金者からのみ送金可能にする仕組みを採用した。また、提案方式では受領者のアカウントを2段階で管理する。外部アカウントと呼ばれる残高管理アカウントでは煩雑な変更を避け、かつ、操作を限定することでセキュリティを堅牢にする一方で、スマートコントラクトを利用して様々な仕様を記載可能とする柔軟な構造を連携される。

提案方式の導入・実装をEthereumの開発者用オープンソースソフトウェアTruffle [6]上で行い、その後、Ganache [2]と呼ばれるテスト用に開発された個人のEthereumブロックチェーン上で提案方式の動作確認、および、導入のオーバーヘッドを計測した。実験の結果、通常の送金手数料が210055 Gas（2023年2月時点の相場で日本円換算で約89円）に対し、提案方式を導入した場合の送金手数料が21999 Gas（同93円）であり、約4.5%の手数料の増加で済むことを確認した。課題2のEthereumブロックチェーン向けの提案方式の実用化に向け、開発したEthereumへの選択的自己防衛方式を論文にまとめIEEEの論文誌へ投稿した。

[課題3]に関する研究成果：

本課題ではBIPとEIPに本研究にて開発した方式を提案するため、開発方式のオーバーヘッドの更なる削減や安全性の評価などの調整を以下の2つの部分課題3.1、3.2に分けて実施した。さら、本研究課題で対象としてきた暗号通貨以外の取引に関する対策への検討を部分課題3.3として実施した。

[部分課題3.1] Bitcoinに関する提案方式のBIP提案に向けた調整

課題1のBitcoinブロックチェーン向けの提案方式の実用化に向け、他の取引やブロックへの影響を調査した結果、提案方式のアドレス型の利用により、取引データ量が増加し、1ブロックに格納可能な取引数が従来アドレス型と比較して40%以上減少することがわかった。この問題を解決するため、Bitcoinで開発されたSegwitと呼ばれるアドレス型の概念を提案アドレスに導入し、課題1で提案したアドレス型を新しいアドレス型に拡張した。この拡張により、1ブロックに格納可能な取引の数をSegwitの概念導入前の2倍以上にまで増加させることができ、オーバーヘッドを改善できることを確認した。

[部分課題3.2] Ethereumに関する提案方式のEIP提案に向けた調整

課題2にて提案したEthereumブロックチェーン向けの方式で利用しているスマートコントラクトと呼ばれるプログラムを搭載可能なアカウントの安全性について考察した。スマートコントラクトはブロックチェーンによって構成される分散台帳に記録されるため、一般の計算機上のプログラムと異なり事後修正ができない。そのため、従来のプログラム以上に実用化の前に注

意深くスマートコントラクトの安全性を検証する必要がある [4]。よって、実現方式の第1段階受領手続きの安全性を検証するため、Ethereum のスマートコントラクトの安全性を検証する複数の安全性検証ツール (Oyente [5], Mythril [1]) を計算環境に導入し、提案手法の当初版と手数料削減を目指した改良版に対して適用した。解析の結果、当初版は安全ではなく、手数料の削減を目指した改良版は安全であることを確認した。さらに、理論的に第2段階受領手続きの安全性を検証した結果、提案手続きでは一般の送金者が選択的自己防衛方式で守られている受領者へ送金を試みた場合、手数料や計算負荷が大きくなってしまいう問題があることがわかった。そこで、提案手続きを改良版し、一般的な送金者が間違っ送金を試みた場合にも、通常送金と計算負荷が大きく変化しないように改良した。

[部分課題 3.3] 暗号通貨以外の取引に関する検討

本研究では主に暗号通貨の送金の受領者未承認取引を防止する自己防衛方式に焦点を置いてきた。しかし、現在、ブロックチェーンでは Non-Fungibility Token (NFT) と呼ばれる暗号通貨以外の暗号資産も取引されている。NFT では画像、動画、不動産権利、プログラムなど様々な形態の資産の取引を扱うことができる。NFT はスマートコントラクトの一部として主に Ethereum ブロックチェーン上で作成され、管理されている。課題 3.2 での調査の結果、我々が開発した Ethereum ブロックチェーンでの自己防衛方式では NFT の受領者未承認取引を完全に防止することが難しいことがわかった。今後、NFT の受領者未承認取引を防止するために、Bitcoin ブロックチェーン向けに開発した自己防衛方式と Ethereum ブロックチェーン向けに開発した自己防衛方式を組み合わせる予定である。

[参考文献]

- [1] ConsensusSysDiligence/mithril, <https://github.com/Consensus/mythril>
- [2] Ganache, <https://trufflesuite.com/ganache>
- [3] libbitcoin, <https://github.com/libbitcoin/libbitcoin>
- [4] L. Luu, D. Chu, H. Olickel, P. Saxena, and A. Hobor, “Making smart contracts smarter,” Proc. of ACM Computer and Communication Security 2016 (CCS’16), pp. 254-269, 2016.
- [5] Oyente, <https://github.com/enzymefinance/oyente>
- [6] Truffle, <https://trufflesuite.com/>

5. 主な発表論文等

〔雑誌論文〕 計0件

〔学会発表〕 計13件（うち招待講演 0件 / うち国際学会 2件）

1. 発表者名 Fusu Zhang, Yoko Kamidoi, Shin'ichi Wakabayashi
2. 発表標題 Enhancing security of generalization methods based on m-invariance for dynamic data publication
3. 学会等名 2024 IEEE 48th Annual International Computer Software and Applications Conference (COMPSAC 2024) (国際学会)
4. 発表年 2024年

1. 発表者名 西村悠生, 上土井陽子, 若林真一
2. 発表標題 IoTシステムのための低計算負荷ユーザ認証の安全性に関する考察
3. 学会等名 2025年 暗号と情報セキュリティシンポジウム (SCIS 2025)
4. 発表年 2025年

1. 発表者名 大野 翔太, 若林 真一, 上土井 陽子
2. 発表標題 多次元データ集合に対するFlexible Distance-based Hashingとk-d木に基づくハイブリッド最近傍探索手法
3. 学会等名 第17回データ工学と情報マネジメントに関するフォーラム (DEIM 2025)
4. 発表年 2025年

1. 発表者名 川崎 允誉, 上土井 陽子, 若林 真一
2. 発表標題 Ethereumブロックチェーンでの受領者未承認取引の防止策について
3. 学会等名 第17回データ工学と情報マネジメントに関するフォーラム (DEIM 2025)
4. 発表年 2025年

1. 発表者名 張 扶蘇、上土井 陽子、若林 真一
2. 発表標題 m-不変性に基づいた連続的データ公開における安全性問題と小規模データ改ざんによる解決法
3. 学会等名 第16回データ工学と情報マネジメントに関するフォーラム(DEIM 2024)
4. 発表年 2024年

1. 発表者名 Chuki Hayama, Yoko Kamidoi, and Shin'ichi Wakabayashi
2. 発表標題 Introduction of a New Method for Preventing Recipient Unapproved Transactions to Bitcoin Wallet
3. 学会等名 2022 IEEE 46th Annual Computers, Software, and Applications Conference (COMPSAC) (国際学会)
4. 発表年 2022年

1. 発表者名 澁川 良輔, 上土井 陽子, 若林 真一
2. 発表標題 ゼロ知識証明に基づく検証可能な秘密分散法の危険性
3. 学会等名 第24回IEEE広島支部学生シンポジウム(HISS2022)
4. 発表年 2022年

1. 発表者名 浜田 凧, 若林 真一, 上土井 陽子
2. 発表標題 移動軌跡データに対する階層的クラスタリングに基づく(k,)-匿名化手法
3. 学会等名 情報処理学会データベースシステム研究会(2022-DBS-176)
4. 発表年 2022年

1. 発表者名 内藤 早紀, 上土井 陽子, 若林 真一
2. 発表標題 Bitcoin Walletでの受領者未承認問題の解決法の実現の課題について
3. 学会等名 2023年暗号と情報セキュリティに関するシンポジウム(SCIS2023)
4. 発表年 2023年

1. 発表者名 張 扶蘇, 上土井 陽子, 若林 真一
2. 発表標題 連続的なデータ公開のためのm-不変性に基づく一般化手法の安全性向上
3. 学会等名 2023年データ工学と情報マネジメントに関するフォーラム(DEIM Forum 2023)
4. 発表年 2023年

1. 発表者名 羽山 宙輝, 上土井 陽子, 若林 真一
2. 発表標題 ビットコインウォレットへの受領者未承認取引の防止策の導入
3. 学会等名 第23回 IEEE 広島支部学生シンポジウム
4. 発表年 2021年

1. 発表者名 浜田 凧, 若林 真一, 上土井 陽子
2. 発表標題 移動軌跡ストリームデータに対して移動ベクトルを利用することで情報損失を低減するリアルタイムk-匿名化手法
3. 学会等名 第23回 IEEE 広島支部学生シンポジウム
4. 発表年 2021年

1. 発表者名 大崎 優也、若林 真一、上土井 陽子
2. 発表標題 高次元データ集合の最近傍探索問題に対するFlexible Distance-based Hashingに基づく厳密解探索手法
3. 学会等名 第14回データ工学と情報マネジメントに関するフォーラム
4. 発表年 2022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
研究分担者	若林 真一 (Wakabayashi Shin'ichi) (50210860)	広島市立大学・情報科学研究科・学長 (25403)	

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
---------	---------