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　６ 年　 ５ 月 ２８ 日現在

機関番号：３２６１２
研究種目：若手研究
研究期間：2018～2023
課題番号：１８Ｋ１８１６２

研究課題名（和文）仮想通貨Bitcoinにおける取引履歴の解析による使用目的の識別と関連性の解明

研究課題名（英文）Research on Bitcoin Transaction Analysis for Digital Forensics

研究代表者
豊田　健太郎（Toyoda, Kentaroh）

慶應義塾大学・理工学部（矢上）・訪問助教

研究者番号：６０７２３４７６

交付決定額（研究期間全体）：（直接経費）　　3,200,000円

研究成果の概要（和文）：Bitcoinは，アドレスと呼ばれる個人と一切紐付けのない口座間で送金が可能な匿名性のある仮想通貨として普及している。この匿名性はマネーロンダリング，違法商品を扱うマーケットプレイスでの決済手段，投資詐欺などに悪用されており、データマイニングを活用し、Bitcoinの取引履歴を解析する手法について取り組んだ。またブロックチェーンの年々増加する取引量増大に伴い、スケーラブルな手法が求められたため、分散機械学習および各データマイニング協力者へのインセンティブ設計、また計算量の少ない取引検証手法についても追加で取り組んだ。本成果は計5通の学術論文誌および5件の国際会議にて発表された。

研究成果の学術的意義や社会的意義
本研究を通じて匿名性の高いデータに対するデータマイニング手法および膨大な取引データの処理などにおいて学術的に意義のある成果を得られた。またBitcoinをはじめとする仮想通貨に関わるエコシステム全体のセキュリティと透明性の向上といった社会的意義も高いと言える。開発した手法は、法執行機関、金融機関、暗号通貨取引所などに応用可能性があり、疑わしい取引の特定と防止に活用できる可能性がある。さらに、提案されたスケーラブルで効率的なデータマイニング技術またインセンティブ・デザインは、仮想通貨のトランザクションデータ分析における新しいアプリケーションやサービスの開発促進に繋がると考えられる。

研究成果の概要（英文）：Bitcoin has gained popularity as an anonymous cryptocurrency that allows for transactions between individuals without any links to their personal identities. This anonymity has been exploited for money laundering, payments on marketplaces for illegal goods, and investment scams known as high-yield investment programs. In this research, we developed a method for analyzing Bitcoin transaction history using data mining techniques. Additionally, we addressed the need for scalable methods due to the increasing transaction volume on the blockchain each year. This involved exploring federatd learning, incentive design for data mining collaborators, and lightweight transaction verification methods. The findings of this research have significant implications for combating illicit activities in Bitcoin. The developed methods will be used by law enforcement agencies, financial institutions, and cryptocurrency exchanges to identify and prevent suspicious transactions.

研究分野：ブロックチェーン

キーワード：ブロックチェーン　フォレンジクス

様　式　Ｃ－１９，Ｆ－１９－１，Ｚ－１９（共通）

１．研究開始当初の背景

近年，Bitcoin は急速に普及し，取引所，ギャンブル，マイクロペイメント，寄付，クラウドファンディング，貸付といった様々な目的に使用されている．その一方で，Bitcoin は一定の匿名性を持つため，犯罪や投資詐欺といった目的に悪用される負の側面もある．

２．研究の目的

そこで本研究では，Bitcoin の取引履歴からさまざまなサービスや犯罪といった使用目的毎に共通する取引の特徴，およびそれらの関連性および類似性を解明した．
この知見に基づき，一定の匿名性のある Bitcoin において，取引の特徴と機械学習を組み合わせることでその使用目的を識別する手法の確立に取り組んだ．
本研究により，Bitcoin を用いた犯罪のフォレンジクスや経済的な側面の解明を可能とし，社会的実用性の高い Bitcoin の解析手法の確立を目指した．

３．研究の方法

主に以下の手順で研究を遂行した．

- 様々なサービス・犯罪に用いられた Bitcoin アドレスの収集
- サービス・犯罪毎の Bitcoin 取引の特徴抽出・識別
- スケーラビリティの課題解決のための分散機械学習，計算量削減手法

４．研究成果

(1) 高利息投資プログラム，および違法商品を扱うマーケットプレイス運営者が管理する Bitcoin アドレスを収集し，それらの取引履歴の特徴を抽出し，教師あり機械学習にて学習・識別を行い，識別精度を評価した．その結果，高利息投資プログラムの識別に関しては，偽陽性率を 5 %程度に抑えつつ，約 95%の識別精度が得られることがわかった．さらに，マネーロンダリング，ギャンブル，高利息投資プログラムなどの計 7 種のクラスに対して多クラス識別を行い，約 73%の正答率で識別できることがわかった．また既存手法は静的な解析がほとんどであり，動的，すなわち時系列解析の手法は例が見られない．そこで Bitcoin アドレスの取引履歴に対して時系列解析ならびに異常検知を行う手法を提案した．提案方式の有効性を示すため，2013 年に米国 SEC (Security and Exchange Commission)に告発された Pirate@40 の投資詐欺に対し提案手法を適用し，取引から算出された異常スコアが実際に起きたイベント時に高くなる傾向があるかを明らかにした．

(2) Bitcoin のブロックチェーン上の取引を統計的機械学習により解析し，さまざまなサービスや犯罪毎に共通する取引の特徴を明らかにし，さらに Bitcoin アドレス毎にそれがどのような目的に使用されたのかを識別する手法の確立に取り組んだ．不当に高い利率を謳った高収益投資プログラム HYIP (High Yield Investment Programs)を Bitcoin によって運営している場合に特化した検知手法についてより詳細な分析を行った．同一ユーザが保持する Bitcoin アドレスを推定するクラスリング手法を活用し，より高い精度で識別が可能な機械学習モデルを得ることに成功し，既存手法で示されていた HYIP 運営者の 32 個のアドレスのうち，提案手法により 30 個を正しく識別することに成功した．2 つ目は，本手法を応用し，ダークネットマーケットの運営者の Bitcoin アドレスを取引履歴の特徴から解析できるかを明らかにした．ダークネットマーケットは匿名通信路(Tor: The Onion Router)のみでアクセス可能なマーケットプレイスであり，主に違法薬物などの売買に使われている．本手法では，インターネット上の掲示板からダークネットマーケットの運営者の Bitcoin アドレスを収集し，それらの含まれる取引履歴をブロックチェーンから取得した．得られた取引履歴から特徴量を抽出し，機械学習によりどの程度識別できるかを評価した．

(3) ブロックチェーンのサイズの増加に伴い，仮想通貨の取引履歴解析を効率的に行うために分散学習を用いるための基盤研究を行った．より正確には，仮想通貨の取引履歴解析の分散学習のためにフェデレーションラーニング (FL:Federated Learning)を用い，さらに参加者もしくは学習協力者に仮想通貨によるインセンティブを配布するメカニズムを提案した．掲載論文においては，コンテスト理論 (contest thoery)と呼ばれるオークション理論の１つを用い，提案メカニズムにより参加者は自身の計算資源およびデータを全て用いることが利得を最大にすること，また最適なインセンティブ分配割合について明らかにした．さらに，これらの知見に基づき，インセンティブメカニズムを考慮したブロックチェーン統合型フェデレーションラーニングに関するサーベイ論文を発表した．

(4) Ethereum ブロックチェーンの処理速度を向上するために, その性能的なボトルネックを明らかにする研究に取り組んだ．多くのユーザが golang で開発された geth と呼ばれるクライアントを用いて Ethereum を起動していることに着目し, pprof と呼ばれる golang の並列処理およびヒープタイムなどを計測するツールおよび自前の関数を用いて明らかにした．複数の同一ネットワークに接続するサーバ上にこれらのツールを配置し，具体的に geth のどの関数がどこでどの程度処理時間を要するかを計測し，geth のボトルネックとなっている点を関数レベルで明らかにした．上記の成果は仮想通貨 Bitcoin における取引履歴の解析をより高速に処理するために極めて重要な成果となった.

(5) Ethereum ブロックチェーンの性能ボトルネックを改善する研究に取り組んだ. 具体的には, sharding および rollups と呼ばれるブロックチェーンの並列処理技術を用いるにあたって, Ethereum アカウントの残高の管理手法および検証に必要なデータサイズをデータ構造およびコミットメントスキームを用いる手法を提案した．さらに KZG (Kate, Zaverucha, Goldberg)コミットメントスキームによるトランザクション検証時の演算量を低減する手法を提案した. 本研究成果は学術論文誌 IEEE Internet-of-Things Journal にて現在査読中である.

これらの成果は，合計 5 通の国際論文誌採録ならびに 4 通の査読付き国際会議論文として対外発表された.

５．主な発表論文等

〔雑誌論文〕　計5件（うち査読付論文　5件／うち国際共著　5件／うちオープンアクセス　5件）

１．著者名 Witt Leon、Heyer Mathis、Toyoda Kentaroh、Samek Wojciech、Li Dan	４．巻 10
２．論文標題 Decentral and Incentivized Federated Learning Frameworks: A Systematic Literature Review	５．発行年 2023年
３．雑誌名 IEEE Internet of Things Journal	６．最初と最後の頁 3642～3663
掲載論文のDOI（デジタルオブジェクト識別子） 10.1109/JIOT.2022.3231363	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 Kudzin Alexander、Toyoda Kentaroh、Takayama Satoshi、Ishigame Atsushi	４．巻 6
２．論文標題 Scaling Ethereum 2.0s Cross-Shard Transactions with Refined Data Structures	５．発行年 2022年
３．雑誌名 Cryptography	６．最初と最後の頁 57～57
掲載論文のDOI（デジタルオブジェクト識別子） 10.3390/cryptography6040057	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 Kentaroh Toyoda; Jun Zhao; Allan Neng Sheng Zhang; P. Takis Mathiopoulos	４．巻 8
２．論文標題 Blockchain-Enabled Federated Learning With Mechanism Design	５．発行年 2020年
３．雑誌名 IEEE Access	６．最初と最後の頁 219744-219756
掲載論文のDOI（デジタルオブジェクト識別子） 10.1109/ACCESS.2020.3043037	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 Kentaroh Toyoda; Koji Machi; Yutaka Ohtake; Allan N. Zhang	４．巻 8
２．論文標題 Function-Level Bottleneck Analysis of Private Proof-of-Authority Ethereum Blockchain	５．発行年 2020年
３．雑誌名 IEEE Access	６．最初と最後の頁 141611-141621
掲載論文のDOI（デジタルオブジェクト識別子） 10.1109/ACCESS.2020.3011876	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 Toyoda Kentaroh、Takis Mathiopoulos P.、Ohtsuki Tomoaki	４．巻 7
２．論文標題 A Novel Methodology for HYIP Operators’ Bitcoin Addresses Identification	５．発行年 2019年
３．雑誌名 IEEE Access	６．最初と最後の頁 74835～74848
掲載論文のDOI（デジタルオブジェクト識別子） 10.1109/ACCESS.2019.2921087	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

〔学会発表〕　計7件（うち招待講演　0件／うち国際学会　4件）

１．発表者名 Kentaroh Toyoda
２．発表標題 Web3 Meets Behavioral Economics: An Example of Profitable Crypto Lottery Mechanism Design
３．学会等名 IEEE International Conference on Metaverse Computing, Networking, and Applications (IEEE MetaCom 2023)（国際学会）
４．発表年 2023年

１．発表者名 Kota Kanemura, Kentaroh Toyoda, Tomoaki Ohtsuki
２．発表標題 Identification of Darknet Markets' Bitcoin Addresses by Voting Per-address Classification Results
３．学会等名 IEEE International Conference on Blockchain and Cryptocurrency (ICBC)（国際学会）
４．発表年 2019年

１．発表者名 Kentaroh Toyoda, Tomoaki Ohtsuki, and P. Takis Mathiopoulos
２．発表標題 Time Series Analysis for Bitcoin Transactions: The Case of Pirate@40's HYIP Scheme
３．学会等名 IEEE International Conference on Data Mining Workshops (ICDMW)（国際学会）
４．発表年 2018年

１．発表者名
Kentaroh Toyoda, Tomoaki Ohtsuki, and P. Takis Mathiopoulos

２．発表標題
Multi-class Bitcoin-enabled Service Identification Based on Transaction History Summarization

３．学会等名
IEEE International Conference on Blockchain（国際学会）

４．発表年
2018年

１．発表者名
金村晃太，豊田健太郎，大槻知明

２．発表標題
アドレス毎の分類結果を用いたダークマーケットの所有するBitcoinアドレス識別

３．学会等名
電子情報通信学会 知的環境とセンサネットワーク研究会（ASN）

４．発表年
2019年

１．発表者名
豊田健太郎，大槻知明，P. Takis Mathiopoulos

２．発表標題
Bitcoinの取引履歴の時系列解析：Pirate@40の高利息投資プログラムの例

３．学会等名
電子情報通信学会 通信方式研究会

４．発表年
2018年

１．発表者名
豊田健太郎，大槻知明，P. Takis Mathiopoulos

２．発表標題
Bitcoinの取引履歴の時系列解析：Pirate@40の高利息投資プログラムの例

３．学会等名
電子情報通信学会 革新的無線通信技術に関する横断型研究会

４．発表年
2018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			
シンガポール	Nanyang Technological University	A*STAR Research Entities		
ギリシャ	University of Athens			