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：３２５０３
研究種目：基盤研究(C)（一般）
研究期間：2020～2022
課題番号：２０Ｋ１１７９７

研究課題名（和文）時空間永続証明システムのためのブロックチェーン基盤技術の開発と偽情報対策への応用

研究課題名（英文）Studies on fundamental blockchain technology for spatio-temporal permanent certification system and its application to countering disinformation

研究代表者
藤原　明広（Fujihara, Akihiro）

千葉工業大学・工学部・教授

研究者番号：７０４４８６８７

交付決定額（研究期間全体）：（直接経費）　　3,400,000円

研究成果の概要（和文）：ブロックチェーン（以降はBCと省略）は取引処理性能が極端に低い問題がある．これを改善するために空間分割したドメイン毎にBCを管理し，BC間に相互運用性を持たせることで取引処理を並列で行う手法を提案した．また既存の相互運用型BCとは異なるチェーンレス型の分散合意アルゴリズムも提案した．これらの提案手法を用いると取引処理性能だけでなくシステムの安全性も改善できることを理論的に示した．
ブロックサイズを増やして取引処理性能を改善するBCプロジェクトが存在する．ブロックサイズを増やした時の取引処理性能や安全性に関する理論を構築した．
またBC技術の偽情報対策への応用としてファクトチェックDAOを提案した．

研究成果の学術的意義や社会的意義
既存の相互運用性を持つBCでは，リレーチェーンを用いて複数のBCを統合管理する共有セキュリティの仕組みを取っている．本研究では，リレーチェーンを用いずに共有セキュリティを強化するチェーンレス型相互運用モデルを提案した．これによりBCの相互運用性に関する新しい研究分野を開拓した．また取引処理性能とシステムの安全性を同時に改善可能なことを理論的に示した点において学術的意義がある．
BC技術の応用としてファクトチェック活動と関連する人材育成を暗号資産（ガバナンストークン）を活用した民主的な投票等によって運営するコミュニティを提案した．ファクトチェック活動の活性化が期待できる点において社会的意義がある．

研究成果の概要（英文）：Blockchain (hereafter abbreviated as BC) has a problem of extremely low transaction processing performance. In order to improve this, we proposed a method for parallel transaction processing by managing BCs in each spatially divided domain and making them interoperable. We also proposed a chainless-type distributed consensus algorithm, which is different from the existing interoperable BCs. We theoretically showed that these proposed methods can improve not only transaction processing performance but also system safety.
There is a BC project to improve transaction processing performance by increasing block size. A theory on transaction processing performance and safety when block size is increased was considered.

We also proposed fact-checking DAO as an application of BC technology to counter disinformation.

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　相互運用性　偽情報対策　DAO

１．研究開始当初の背景

ブロックチェーン（以降BCと省略）は1990年台にHaberとStornettaによって発表された電子書類の分散タイムスタンプ・サービスの理論研究[1,2]に起源がある．当時はインターネットが現在ほど発達していなかったが，2008年にビットコインが登場する頃には環境が整っていたため，翌2009年から実験的な稼働が始まった．それ以来，今日まで10年以上の期間，稼働が継続している．一方，ビットコインのWhite PaperにはElectronic Cash Systemを実現しているように書かれているが，現状のビットコインをはじめとするBCシステムでは普段から使える現金(Cash)を実現できていない．この理由としては，BCシステムでは匿名性と実時間性が実現できていないことが挙げられる．匿名性は利用者のプライバシーを保護する観点から重要である．また実時間性を実現するためには取引処理速度の性能を向上させる必要がある．

本研究を開始した当初は，匿名性を実現する技術の研究も行う予定であった．しかし，その後の調査によってビットコインは意図的に匿名性を排除した設計になっていることを理解した．現状の暗号資産の一部は，悪事で稼いだお金の資金洗浄やテロ資金供与に利用されていることが知られている[3]．匿名性を実現しようとすると，これらの悪事をはたらくことが容易になるという問題が生じる．BCは誰でも閲覧可能であるため，悪事を働いたお金の取引は自然と注目され，追跡される．この特徴を利用して，悪事をはたらく動機を排除しようとする設計になっている．上記の理由により，匿名性の研究は暗号資産の悪用に関する調査に留め，主に取引処理性能の向上に焦点を絞って研究を進めることとした．

BC技術を偽情報対策に応用することについても検討した．最近，Stable DiffusionやChatGPTなどの生成AI技術が注目を集めている．一方，AlexNet等の開発を通じて今日のディープラーニングのブームを作ったHinton教授が，生成AI技術の悪用についての懸念を表明している．その中で，生成AIは「皆が何が本当か分からないようなフェイクニュースを大量に生成されてしまうリスクがある」と指摘している[4]．このように生成AI技術が急速に身近なものになってきていいる昨今，偽情報対策は喫緊の課題である．フェイクニュースに対抗するためには，人間側の情報リテラシを向上させることが有効であることが指摘されている[5]．一方，日本では海外と比較べてファクトチェック活動を行っている団体が少ないなど，活動があまり活発でないことも知られている[6]．真偽検証を行うファクトチェッカーの人材の不足，ファクトチェック活動に対する報酬を得る仕組みが未発達であること，文化的要因の違いなど，様々な原因が考えられる

２．研究の目的

本研究ではBCの取引処理性能を向上させるために，BC間の相互運用性を利用する方法とブロックサイズを増加させる方法の二つの手法に着目し，それらの有効性を理論と実験の両方の観点から探る．また，取引処理性能を評価するための基礎理論を構築する．またBCの偽情報対策への応用として，分散型自律組織(Decentralized Autonomous Organization, DAO)を用いることで，ファクトチェッカーの人材不足を解消したり，ファクトチェック活動を活性化させるコミュニティの可能性について考える．

３．研究の方法

BC間の相互運用性については，既存の相互運用型BCでよく用いられているリレチェーンによる共有セキュリティを超える分散型合意アルゴリズムの開発を行う．通常のブロック部に加えて，共有ブロック部を追加し，複数のBCでの合意情報を各BCに記録する機構を採用することで，取引処理性能や安全性に与える影響について調査する．ブロックサイズを増加させた時の取引処理性能に関する数理モデルを考案し，理論的な取引処理性能の限界について調査する．ファクトチェックDAOを提案し，ファクトチェックコンテ

ストを開催する．コンテストの前後にアンケートを取ることで，DAOを用いた手法の有効性を調査する．

４．研究成果

(1) チェーンレス型BC相互運用性

ビットコインが登場して以来，さまざまなBCプロジェクトが提案されてきた．異なるBC間で仮想資産を自由に交換する需要の増加に伴い，複数のBC間で相互にオンチェーン情報を読み書き可能な特性としてのクロスチェーン相互運用性を実現することが重要になってきている．一方，パブリックBCには取引処理能力が非常に遅いというスケーラビリティの問題がある．クロスチェーン相互運用性を高めることがスケーラビリティ問題に与えるインパクトについて検討した．PolkadotやCosmosといった既存の相互運用型BCプロジェクトに比べて，より非中央集権性が高い特性を持つチェーンレス多層コンセンサスを提案した．実装したノードプログラムを用いていくつかの実験を行い，コンセンサスを得るために必要な遅延時間を評価した．100以上のパラチェーンで構築した大規模ネットワークを用いた実験の結果，並列に取引処理を行った時の遅延時間が，パラチェーン数の増加と共に超線形で増加する傾向を確認した．この結果により実用的な取引処理能力を実現しつつ，チェーンレス型の相互運用モデルを安全に実行するために必要なBCの設定を確認することができた．

[本研究に関する主な発表論文]

[1] T. Yanagihara & A. Fujihara, “Considering Chainless Interoperabilityacross Many Parachains” IEEE ICBC 2023, Crosschain Workshop, to appear (2023).

[2] T. Yanagihara & A. Fujihara, “Cross-Referencing Method for ScalablePublic Block-chain” Internet of Things, Vol. 15, 100419, Elsevier (2021).

(2)ブロックサイズの増加が取引処理性能に与える影響

Bitcoin SV スケーリング・テスト・ネットワーク(STN)は，オンチェーン技術を駆使したBitcoinの取引処理能力を性能評価するための実験的なネットワークである．大量のトランザクションが，常にピア・ツー・ピアネットワークに送信され，1GBを超える巨大なブロックが頻繁に生成されている．

本研究では，STNノードを実行することにより，取引処理の待ち行列の稼働率とBCの分岐確率を推定したその結果，推定稼働率は約1.04と1を超えていることが分かった．また推定BC分岐確率は8.5%となり，既存のビットコインの分岐確率と比べて，とても大きくなっていることが分かった．

またIoTノードが得たデータをBCに記録する応用を想定して，OP_RETURNスクリプトを含む取引を1分に1回の頻度で，1週間に渡って送信し続ける実験を行い，取引が承認される確率を実験的に評価した．その結果取引の承認確率は98%になった．また取引が承認されるまでにかかる待ち時間の分布の裾野が冪分布に従うことも確認した．これらの結果から，STNは優先権付き待ち行列モデルにしたがって分析可能であることが分かった．

[本研究に関する主な発表論文]

[3] A. Fujihara & T. Yanagihara, “Performance Evaluation Experiments of Bitcoin SV Scaling Test Network” Advances in Intelligent Networking and Collaborative Systems, Lecture Notes In Networks and Systems, Vol. 527, Springer (2022).

(3) ファクトチェックDAOの提案

近年の急速なインターネットの普及により，誰もが自由に意見を発信できる反面，フェイクニュースなどの疑義言説の影響が社会問題となっている．この対処法として，疑義言説を真偽検証するファクトチェック活動が注目を集めている．しかし，その活動の大半は無償で行われている．また，一般の人達が

ファクトチェッカーを応援する仕組みやファクトチェックに参加する仕組みも未成熟である．

本研究では，これらの問題を解決するためにファクトチェック DAO を提案した．DAOとは，日本語では分散型自律組織と呼ばれる，暗号資産を利用した民主的な投票等を活用した運営を行うコミュニティのことである．実際にWeb3アプリを試作し，フ ァクトチェックコンテストを開催することで，アプリが参加者に与える影響について評価した．コンテスト前後でアンケ ート調査を行うことにより，ファクトチェックに対する感情の変化やアプリを用いたファクトチェック活動の持続可能性について考察した．その結果，コンテスト後にファクトチェックに対する関心が若干向上したことと，ファクトチェック活動を持続可能にする報酬の推定を行うことができた．

[本研究に関する主な発表論文]

[4] 中沢遼輔，藤原明広，ファクトチェックDAOの提案，信学技報，vol．122，no．407，IN2022-115，pp．293-298（2023）．

参考文献

[1] S. Haber and W. S. Stornetta, “Secure Names for Bit-Strings,” CCS’97: Proceedings of the 4th ACM conference on Computer and communications security, pp. 28-35 (1997).

[2] CoinGeek, “Stuart Haber & Scott Stornetta: How our timestamping mechanism was used in Bitcoin | CGConversations” https://www.youtube.com/watch?v=WWVoPBkPd6g（2023年6月8日閲覧確認）

[3] CFLW, “RAND used Dark Web Monitor for strategic insight Zcash use” https://cflw.com/2020/05/06/rand-used-dark-web-monitor-for-strategic-insight-zcash-use/（2023年6月8日閲覧確認）

[4] PBS NewsHour, ‘Godfather of AI’ discusses dangers the developing technologies pose to society https://www.youtube.com/watch?v=yAgQWnD3lnE（2023年6月8日閲覧確認）

[5] lifehacker, フィンランドのメディアリテラシー教育に学ぶ、フェイクニュースの見分け方（2019）https://www.lifehacker.jp/article/195010-how-to-learn-media-literacy-to-take-measures-to-fake-news/（2023年6月8日閲覧確認）

[6] 楊井人文，日本のファクトチェック活動は活性化したか（2022）https://www.fij.info/archives/10713 （2023年6月8日閲覧確認）

５．主な発表論文等

〔雑誌論文〕　計5件（うち査読付論文　4件／うち国際共著　0件／うちオープンアクセス　2件）

１．著者名 Yanagihara Takaaki、Fujihara Akihiro	４．巻 15
２．論文標題 Cross-Referencing Method for Scalable Public Blockchain	５．発行年 2021年
３．雑誌名 Internet of Things	６．最初と最後の頁 100419～100419
掲載論文のDOI（デジタルオブジェクト識別子） 10.1016/j.iot.2021.100419	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 －

１．著者名 Amita Shogo、Fujihara Akihiro	４．巻 53999
２．論文標題 A Performance Evaluation of Vehicular Swarm Intelligence for Seamless Route Guidance using Opportunistic Networking	５．発行年 2021年
３．雑誌名 IEEE Xplore	６．最初と最後の頁 8
掲載論文のDOI（デジタルオブジェクト識別子） 10.1109/CANDARW53999.2021.00008	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 Takaaki Yanagihara, Akihiro Fujihara	４．巻 65
２．論文標題 Considering Cross-Referencing Method for Scalable Public Blockchain	５．発行年 2021年
３．雑誌名 Advances in Internet, Data and Web Technologies	６．最初と最後の頁 220-231
掲載論文のDOI（デジタルオブジェクト識別子） 10.1007/978-3-030-70639-5_21	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 Fujihara Akihiro	４．巻 16
２．論文標題 「ブロックチェーン」を学んで，使ってみよう！	５．発行年 2022年
３．雑誌名 IEICE Communications Society Magazine	６．最初と最後の頁 30～37
掲載論文のDOI（デジタルオブジェクト識別子） 10.1587/bplus.16.30	査読の有無 無
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 －

１．著者名 Fujihara Akihiro、Yanagihara Takaaki	４．巻 527
２．論文標題 Performance Evaluation Experiments of Bitcoin SV Scaling Test Network	５．発行年 2022年
３．雑誌名 Advances in Intelligent Networking and Collaborative Systems	６．最初と最後の頁 150～160
掲載論文のDOI（デジタルオブジェクト識別子） 10.1007/978-3-031-14627-5_15	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25件（うち招待講演　4件／うち国際学会　6件）

１．発表者名 Takaaki Yanagihara and Akihiro Fujihara
２．発表標題 Considering Chainless Interoperability across Many Parachains
３．学会等名 IEEE ICBC 2023（国際学会）
４．発表年 2023年

１．発表者名 Akihiro Fujihara and Takaaki Yanagihara
２．発表標題 Performance Evaluation Experiments of Bitcoin SV Scaling Test Network
３．学会等名 The 14th International Conference on Intelligent Networking and Collaborative Systems (INCoS-2022)（国際学会）
４．発表年 2022年

１．発表者名 柳原貴明，藤原明広
２．発表標題 ブロックチェーン履歴交差法の実験的性能評価
３．学会等名 情報ネットワーク研究会
４．発表年 2020年

１．発表者名
柳原貴明，藤原明広

２．発表標題
連合型合意の提案と多数ノードによる性能評価実験

３．学会等名
ネットワークシステム研究会

４．発表年
2022年

１．発表者名
柳原貴明，藤原明広

２．発表標題
チェーンレス型多層合意における待ち時間の実験的評価

３．学会等名
ネットワークシステム研究会

４．発表年
2022年

１．発表者名
柳原貴明，藤原明広

２．発表標題
チェーンレス型多層合意の安全性とセキュリティに関する考察

３．学会等名
ネットワークシステム研究会

４．発表年
2023年

１．発表者名
中沢遼輔，藤原明広

２．発表標題
ファクトチェックDAOの提案

３．学会等名
情報ネットワーク研究会

４．発表年
2023年

１．発表者名
櫻井柾希・藤原明広

２．発表標題
ビットコインを用いたファクトチェック・レジストリの実装

３．学会等名
情報ネットワーク研究会

４．発表年
2023年

１．発表者名
Akihiro Fujihara

２．発表標題
Harmonization of competition and cooperation in consensus algorithm: Toward a solution to blockchain scalability problem

３．学会等名
IEEE ICCCI 2022（招待講演）（国際学会）

４．発表年
2022年

１．発表者名
Akihiro Fujihara

２．発表標題
Theoretical Considerations on Bitcoin Block Size Distribution

３．学会等名
Blockchain Kaigi 2022 (BCK22)（国際学会）

４．発表年
2022年

１．発表者名
柳原貴明・藤原明広

２．発表標題
連合型合意の提案と多数ノードによる性能評価実験

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
2022年

１．発表者名
柳原貴明・藤原明広

２．発表標題
チェーンレス型多層合意における待ち時間の実験的評価

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
2022年

１．発表者名
柳原貴明・藤原明広

２．発表標題
チェーンレス型多層合意の安全性とセキュリティに関する考察

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
2022年

１．発表者名
中沢遼輔・藤原明広

２．発表標題
ファクトチェックDAOの提案

３．学会等名
電子情報通信学会　情報ネットワーク研究会

４．発表年
2022年

１．発表者名
櫻井柾希・藤原明広

２．発表標題
ビットコインを用いたファクトチェック・レジストリの実装

３．学会等名
電子情報通信学会　情報ネットワーク研究会

４．発表年
2022年

１．発表者名
Akihiro Fujihara

２．発表標題
Harmonization of competition and cooperation in consensus algorithm: Toward a solution to blockchain scalability problem

３．学会等名
2022 4th International Conference on Computer Communication and the Internet 2022（招待講演）

４．発表年
2022年

１．発表者名
Akihiro Fujihara

２．発表標題
Theoretical Considerations on Bitcoin Block Size Distribution

３．学会等名
Blockchain Kaigi 2022 (BCK22)

４．発表年
2022年

１．発表者名
Akihiro Fujihara and Takaaki Yanagihara

２．発表標題
Performance Evaluation Experiments of Bitcoin SV Scaling Test Network

３．学会等名
The 14th International Conference on Intelligent Networking and Collaborative Systems (INCoS-2022)

４．発表年
2022年

１．発表者名
Akihiro Fujihara

２．発表標題
On-chain Scaling of Blockchain

３．学会等名
2021 Japan-America Frontiers of Engineering Symposium (JAFOE)（招待講演）（国際学会）

４．発表年
2021年

１．発表者名
Takaaki Yanagihara, Akihiro Fujihara

２．発表標題
Considering Cross-Referencing Method for Scalable Public Blockchain

３．学会等名
International Conference on Emerging Internetworking, Data & Web Technologies (EIDWT) 2021（国際学会）

４．発表年
2021年

１．発表者名
藤原明広

２．発表標題
人との接触機会に関する研究とその応用に向けた課題

３．学会等名
2021年電子情報通信学会総合大会（招待講演）

４．発表年
2021年

１．発表者名
藤原明広

２．発表標題
ビットコインスケーリングテストネットワーク性能評価実験

３．学会等名
情報ネットワーク研究会

４．発表年
2021年

１．発表者名
加藤豊，藤原明広

２．発表標題
ブロックチェーンにおけるオラクル問題の集合知を用いた回避に関する実験的性能評価

３．学会等名
情報ネットワーク研究会

４．発表年
2021年

１．発表者名
網田昇悟，藤原明広

２．発表標題
近接情報共有型交通車両群誘導法の性能評価 ～ 近接情報共有型車両の割合の影響 ～

３．学会等名
情報ネットワーク研究会

４．発表年
2021年

１．発表者名
藤原明広

２．発表標題
ビットコインのブロックサイズ分布とその理論的考察

３．学会等名
社会物理学研究会

４．発表年
2021年

〔図書〕　計0件

〔産業財産権〕

〔その他〕

藤原明広のウェブページ Akihiro Fujihara's Webpage
https://sites.google.com/site/akihirofujihara/

Open BlockChain
https://blockchain.open.ac.uk/#covid-19

Consensus Algorithms for Scalable Public Blockchains
https://www.frontiersin.org/research-topics/35586/consensus-algorithms-for-scalable-public-blockchains

Ichigo-Ichie: Life Logging and Exposure Notification
https://www.ted.com/talks/akihiro_fujihara_ichigo_ichie_life_logging_and_exposure_notification
https://www.youtube.com/watch?v=E-jpINKQ_Vo

ブロックチェーンは世界を変えるテクノロジー、ただしスケーラビリティやオラクルなど課題は山積み
https://meta-bank.jp/theme/fujihara-professor/

「ブロックチェーン」を学んで使ってみよう！
https://www.jstage.jst.go.jp/article/bplus/16/1/16_30/_pdf

2021 Japan-America Frontiers of Engineering Symposium
https://www.naefrontiers.org/196650/Akihiro-Fujihara

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
研究協力者	柳原　貴明 (YANAGIHARA Takaaki)	千葉工業大学・大学院工学研究科 (32503)	

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