日本学術振興会に紙媒体で提出する必要はありません。

4版

様　式　C－7－1

令和２年度科学研究費助成事業（科学研究費補助金）実績報告書（研究実績報告書）

機関番号	１４６０３

所属研究機関名称		奈良先端科学技術大学院大学
研究代表者	部局	先端科学技術研究科
	職	教授
	氏名	笠原　正治

１．研究種目名　基盤研究(A)(一般)　　２．課題番号　19H01103

３．研究課題名　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

４．研究期間　令和元年度～令和４年度　　５．領域番号・区分　－

６．研究実績の概要

(1)ビットコインにおけるBWH攻撃のゲーム理論的分析
ビットコインでは，複数のマイナーノードがマイニングプールと呼ばれるグループを形成してハッシュ計算を協力して行っている．参加ノードに対する報酬は貢献度に応じて配分されるため，マイナーノードは大きい収益が期待できるマイニングプールを選択しようとする．一方，マイニングプールレベルのセキュリティ問題として，マイナーをスパイとしてプールに潜入させ，ブロックを発見してもプール管理者に通知しない形でマイニングを妨害するBlock Withholding (BWH)攻撃が知られている．ここではBWH攻撃が存在する状況下でのマイナーのプール選択問題について，プール数が二つの場合に着目し，進化ゲーム理論を用いてマイナーノード人口の時間推移を分析するモデルを検討した．計算機シミュレーションより，進化的に安定となる戦略の存在を確認するとともに，スパイ・マイナーのハッシュレートが相対的に小さい場合でも攻撃対象プールの収益を低下させ，攻撃側のプールのマイナー人口が増加することが確認された．
(2)有向非巡回グラフ構造を持つ分散台帳技術を応用したIoTアクセス制御技術
莫大な数のIoTデバイスがネットワーク接続されたIoTシステムに対する分散台帳技術として，IOTAフレームワークがある．IOTAでは，Tangleと呼ばれる有向非巡回グラフ構造を持ったデータ構造でトランザクションを保持する．ここでは公開鍵暗号方式の一種であるCP-ABE方式に着目し，CapBACとABACを組み合わせたアクセス制御方式の提案を行った．提案方式では，サブジェクトとその所有者の間に安全な通信路を必要とせず，1対多のアクセス制御を提供できる．提案方式の実行可能性を検証するため，プロトタイプの実装を行い，権限の付与や検証の機能に対する実証実験を通じて提案方式の実行可能性を確認した．

７．キーワード

ブロック・チェーン　DSSトリレンマ　低遅延P2Pネットワーク　高速ブロック同期　IoTアクセス制御

８．現在までの進捗状況

区分　(2) おおむね順調に進展している。

理由
本年度は(1)ビットコイン・ブロック・チェーンにおけるセキュリティ脆弱性，(2) 有向非巡回グラフ構造を持つ分散台帳技術を応用したIoTアクセス制御技術，(3) ZDDによるグラフ列挙アルゴリズムの高速化手法と応用，の三点を中心に検討を進め，順調に研究が進展している．
(1) ブロック・チェーンにおけるセキュリティ脆弱性問題としてBWH攻撃に着目し，進化ゲーム理論を用いてマイナー人口の推移を分析した．また，マイナーノードのプール選択を強化学習で行わせる状況を考え，Q学習，DQN，A2Cの3種類のアルゴリズムについて計算機シミュレーションによる特性評価を行った．
(2) IOTAの従来研究では，MAMと呼ばれるプロトコルを活用したアクセス制御方式が提案されているが，サブジェクトとその所有者の間に安全な通信路が必要であり，1対1のアクセス制御に限定されているといった欠点があった．ここではCP-ABEと呼ばれる公開鍵暗号方式に着目し，CapBACとABACを組み合わせたアクセス制御方式を提案した．提案方式では，サブジェクトと所有者の間に安全な通信路を必要とせず，1対多のアクセス制御を提供できる．提案方式の実行可能性を検証するため，プロトタイプの実装を行い，権限の付与や検証の機能に対する実証実験を通じて提案方式の実行可能性を確認した．
(3) ZDDを用いて部分グラフを列挙する手法としてフロンティア法がある．ここではフロンティア法の高速化手法としてビームサーチと局所探索による変数順序付けを工夫した手法を検討し，サイズの大きいグラフに対する列挙問題に対して従来法よりも効率よく処理できることを計算機実験により確認した．また，ZDDが取り扱えるグラフクラス拡張のため，メニエルグラフと交差弦グラフと呼ばれるクラスに着目し，ZDDを構築するアルゴリズムの提案とその有効性に対する検証を行った．

日本学術振興会に紙媒体で提出する必要はありません。

９．今後の研究の推進方策

(1)ビットコインでは一部のマイナーノードがトランザクション手数料による優先処理を行なっていることが知られている．一方，最近の関連研究において，手数料がブロック・チェーンの安全性にも影響を与える可能性があることが報告されている．ここでは過去に検討した待ち行列モデルを発展させ，ブロック承認における合意形成アルゴリズムを考慮した，トランザクション手数料とセキュリティの脆弱性の関係を分析する数理モデルの検討を行う．具体的には，トランザクション手数料とマイナーノードの参加離脱行動の関係性をゲーム理論によって定式化し，ブロック・チェーンのセキュリティに対する手数料の影響を表現する数理モデルを提案するとともに，高い安全性を保証しつつ高スループットを実現する手数料の決定方法についても検討を行う．
(2)ブロック・チェーンの合意形成アルゴリズムとして，投票に基づいてブロックの正当性を検証するProof-of-Stake (PoS)がある．PoSでは，不正な投票が増大すると適切な合意形成ができなくなるため，参加ノードに正しい投票を行わせるインセンティブ・メカニズムが重要である．ここでは参加ノードの投票結果に対して投票履歴を考慮して報酬・罰則を与える方式，及び罰則で回収したトークンを再配布するメカニズムについても検討を行う．
(3) Ethereum上でIoTデバイスが生成する大量のデータを蓄積しようとすると，管理処理に高いコストがかかることが知られている．一方，データをオフチェーン型のデータ構造として取り扱う方式としてオラクルと呼ばれる技術がある．このブロック・チェーン・オラクル技術に着目し，大規模IoTネットワーク上で大量に処理されるデータの効率的な利用に向けたオラクルベースのメインチェーン・オフチェーン結合アーキテクチャを検討し，プロトタイプを実装して提案方式の実現可能性を検討する．

１０．研究発表（令和２年度の研究成果）

〔雑誌論文〕　計7件（うち査読付論文　7件／うち国際共著論文　0件／うちオープンアクセス　3件）

１．著者名 Fujita Kentaro、Zhang Yuanyu、Sasabe Masahiro、Kasahara Shoji	４．巻 11
２．論文標題 Mining Pool Selection under Block WithHolding Attack	５．発行年 2021年
３．雑誌名 Applied Sciences	６．最初と最後の頁 1617～1617
掲載論文のDOI（デジタルオブジェクト識別子） 10.3390/app11041617	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 Hara Takanori、Sasabe Masahiro、Kasahara Shoji	４．巻 1
２．論文標題 Selfish Yet Optimal Routing by Adjusting Perceived Traffic Information of Road Networks	５．発行年 2020年
３．雑誌名 IEEE Open Journal of Intelligent Transportation Systems	６．最初と最後の頁 120～133
掲載論文のDOI（デジタルオブジェクト識別子） 10.1109/0JITS.2020.3019935	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 Hara Takanori、Sasabe Masahiro、Matsuda Taiki、Kasahara Shoji	４．巻 9
２．論文標題 Capacitated Refuge Assignment for Speedy and Reliable Evacuation	５．発行年 2020年
３．雑誌名 ISPRS International Journal of Geo-Information	６．最初と最後の頁 442～442
掲載論文のDOI（デジタルオブジェクト識別子） 10.3390/ijgi9070442	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 Nishi Yohei、Sasabe Masahiro、Kasahara Shoji	4．巻 13
2．論文標題 Optimality analysis of locality-aware tit-for-tat-based P2P file distribution	5．発行年 2020年
3．雑誌名 Peer-to-Peer Networking and Applications	6．最初と最後の頁 1688～1703
掲載論文のDOI（デジタルオブジェクト識別子） 10.1007/s12083-020-00925-2	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 －

1．著者名 Qu Qianyue、Zhang Yuanyu、Kasahara Shoji	4．巻 -
2．論文標題 On Eavesdropping Region Characterization in Hybrid Wireless Communications	5．発行年 2020年
3．雑誌名 2020 International Conference on Networking and Network Applications (NaNA2020)	6．最初と最後の頁 29-34
掲載論文のDOI（デジタルオブジェクト識別子） 10.1109/NaNA51271.2020.00013	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 Fujita Kentaro、Zhang Yuanyu、Sasabe Masahiro、Kasahara Shoji	4．巻 -
2．論文標題 Mining Pool Selection Problem in the Presence of Block Withholding Attack	5．発行年 2020年
3．雑誌名 The 3rd IEEE International Conference on Blockchain (Blockchain-2020)	6．最初と最後の頁 329-334
掲載論文のDOI（デジタルオブジェクト識別子） 10.1109/Blockchain50366.2020.00047	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 Nakanishi Ruka、Zhang Yuanyu、Sasabe Masahiro、Kasahara Shoji	4．巻 -
2．論文標題 IOTA-Based Access Control Framework for the Internet of Things	5．発行年 2020年
3．雑誌名 The 2nd conference on Blockchain Research and Applications for Innovative Networks and Services (BRAINS'20)	6．最初と最後の頁 87-95
掲載論文のDOI（デジタルオブジェクト識別子） 10.1109/BRAINS49436.2020.9223293	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6件（うち招待講演　1件／うち国際学会　2件）

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 松永赳尭，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

〔図書〕　計0件

１１．研究成果による産業財産権の出願・取得状況

計0件（うち出願0件／うち取得0件）

１２．科研費を使用して開催した国際研究集会

計0件

１３．本研究に関連して実施した国際共同研究の実施状況

―

１４．備考

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/