日本学術振興会に紙媒体で提出する必要はありません。

様　式　Ｆ－７－１

科学研究費助成事業（学術研究助成基金助成金）実施状況報告書（研究実施状況報告書）（令和元年度）

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	准教授
	氏名	笹部　昌弘

１．研究種目名　基盤研究(C)(特設分野研究)　　２．課題番号　19KT0045

３．研究課題名　Bitcoin型競争的情報拡散に基づく合意形成における情報拡散妨害のリスク分析

４．補助事業期間　令和元年度～令和３年度

５．研究実績の概要

暗号通貨システムBitcoinでは，悪意のあるユーザを含む不特定多数のユーザ間での取引台帳（ブロックチェーン）に対する自律分散合意形成を実現している．新たなブロック（取引情報の集まり）の生成はマイナーと呼ばれる特別な端末により行われるが，その際，過去のブロック情報と高難度なパズル的計算が必要となる．また，ブロックチェーンの追記に成功したユーザのみがシステムと取引利用者から報酬を得られる．その結果，ネットワークを介したユーザ間での情報拡散競争とブロック生成競争が発生し，これがブロックチェーンの耐改竄性に寄与している．
ここで，情報の正常な拡散はブロックチェーンの信頼性実現に必須となるが，Bitcoinプロトコルで採用されているプル型情報伝播に対するタイムアウト制御の悪用により，隣接端末間の情報伝播の妨害が比較的容易に実現できることが知られている．本研究では，特定のマイナーが複数の攻撃者と結託し，競合するマイナーの生成したブロックの拡散を妨害する，ブロック拡散妨害攻撃という新たなリスクに着目している．
本年度では，ブロック拡散妨害攻撃の基本特性の分析のために，感染症伝播モデルに着想を得た新たな数理モデルを確立した．さらに，より詳細な分析のために，Bitcoinプロトコル及びブロック拡散妨害を再現したシミュレータを開発した．解析とシミュレーション評価により，攻撃者の数や位置，ネットワークの形状がブロック拡散妨害攻撃のリスクに与える影響を明らかにした．

６．キーワード

競争的情報拡散　Bitcoin　情報拡散妨害　リスク分析　感染症伝播モデル

７．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
研究は概ね順調に進んでおり，得られた研究成果の一部は，国際会議1件，研究会4件の形で対外的に発表している．特に，国際会議では招待講演，研究会の内1件は依頼講演の形でそれぞれ実施しており，対外的にも研究の重要性が認知されつつある．

日本学術振興会に紙媒体で提出する必要はありません。

3版

８．今後の研究の推進方策

今後の研究の推進に向けては大きく二つの方策を想定している．一つ目は，数理モデルの拡張である．初年度に確立した数理モデルでは，同一の攻撃者から複数回攻撃を受ける可能性を含む形となっており，これは拡散妨害の最大リスクの評価に対応する．一方，Bitcoinシステムでは，各ノードが他のノードとの過去の通信履歴を保持できる．この点を考慮し，同一攻撃者からの攻撃受信回数を高々1回に抑えた場合の数理モデルを新たに確立し，そのリスク評価を行う．
二つ目は，拡散妨害攻撃への対策の検討である．初年度においてもその検討を一部開始しているが，攻撃への対策としては，攻撃からの早期復旧と攻撃の回避の両面から取り組む必要がある．前者には，迅速なブロック取得と攻撃の早期検出を両立するための適切なタイムアウト制御が，後者には，ブロックの生成・拡散が継続的に行われる特性に着目した，過去の通信履歴に基づく適切な取得先ノードの選択がそれぞれ重要な役割を担うものと期待される．

９．次年度使用が生じた理由と使用計画

導入を予定していた計算機の発売時期の遅れによるものであり，次年度中にその購入費用の一部に充てる予定である．

１０．研究発表（令和元年度の研究成果）

〔雑誌論文〕　計0件

〔学会発表〕　計5件（うち招待講演　1件／うち国際学会　1件）

１．発表者名
Masahiro Sasabe

２．発表標題
Interruption Risk of Competitive Block Diffusion in a Bitcoin Network

３．学会等名
Workshop on Internet Architecture and Applications（招待講演）（国際学会）

４．発表年
2019年

１．発表者名
笹部 昌弘

２．発表標題
Bitcoinネットワークにおけるブロック拡散妨害の数理モデル化

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
2019年

日本学術振興会に紙媒体で提出する必要はありません。

1．発表者名 笹部 昌弘
2．発表標題 Bitcoinネットワークにおけるブロック拡散妨害の感染症伝播モデルに着想を得た数理モデル化
3．学会等名 超知性ネットワーキングに関する分野横断型研究会
4．発表年 2019年

1．発表者名 山本 将成，笹部 昌弘，笠原 正治
2．発表標題 ビットコインネットワークにおけるブロック拡散妨害攻撃のリスク評価
3．学会等名 電子情報通信学会コミュニケーションクオリティ研究会
4．発表年 2019年

1．発表者名 山本 将成，笹部 昌弘，笠原 正治
2．発表標題 ビットコインネットワークにおけるブロック拡散妨害攻撃への対抗策 ～ 推定ダウンロード速度に基づくブロック取得先選択 ～
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 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

―