

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２年度）

所属研究機関名称			機関番号	1 4 6 0 3
研究 代表者	部局	奈良先端科学技術大学院大学		
	職	先端科学技術研究科		
	氏名	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型競争の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、悪意のあるユーザが存在したとしても不特定多数のユーザ間で自律分散的にブロックチェーン（取引台帳）に対する合意を形成できる。この合意形成は、ユーザ間でのブロック生成・拡散に関する二つの競争的原理により実現される。ブロック生成競争は高難度のバズルの計算を要する計算力の競争となる一方、ブロック拡散競争は、システムを構成するノード間で形成されたネットワーク上での情報拡散速度に依存する。Bitcoinではブロックサイズが1 MB程度と比較的大きいため、隣接ノード間のブロック伝播時に、まず受信先にメタ情報のみを送信する。受信先はメタ情報を基に未所持のブロックのみ取得を試みる。しかしながら、このプル型情報伝播では、自身の隣接ノードにメタ情報のみを送信し、その後のブロックの要求を無視することでブロック伝播を妨害できる脆弱性が存在する。本研究では、複数の攻撃者が結託し、ブロック伝播妨害を同時に行うブロック拡散妨害のリスクに着目している。今年度は、このようなネットワーク上での競争の情報拡散とその妨害の様子を、感染症伝播モデルに着想を得たNetwork SIRAモデルとして新たに確立した。初年度の検討では、任意の2ノードが均一な確率で通信可能であるという前提の下でのモデルの基本形をScalar SIRAモデルとして確立しており、このモデルを用いた評価により、ノード間の通信確率、通常のブロック伝播速度、ブロックの妨害速度などのシステムパラメタが拡散妨害リスクに与える影響を明らかにしている。今年度は、このモデルを、ネットワーク上での競争の情報拡散とその妨害の様子を表す、Network SIRAモデルへと拡張するとともに、数値評価により、ネットワークの形状とネットワーク上での攻撃者の位置が拡散リスクに与える影響を明らかにした。

6．キーワード

競争的信息拡散 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
ネットワーク上でのブロック拡散妨害攻撃のモデル化と定量的なリスク評価の観点で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、Elsevier社のComputer Networksに雑誌論文として掲載されている。

2 版

8．今後の研究の推進方策

これまでの検討で確立した2種類のSIRAモデル（Scalar SIRAモデルとNetwork SIRAモデル）を用いた数値評価により、競争的情報拡散における拡散妨害攻撃のリスクが明らかとなっている。特に、隣接ノード間での攻撃（妨害）は情報（ブロック）のメタ情報の送信により実現可能となるため、情報本体と比較してメタ情報のサイズが小さくなるほど攻撃のリスクが高まる。また、ネットワーク構造が不均質な場合、ハブと呼ばれる高次数ノードが攻撃者になると拡散妨害リスクが急激に高まる。

そのため、拡散妨害攻撃への対策手法の確立が重要となる。攻撃への対策としては、万一、攻撃を受けた場合においても早期に復旧できるための仕組みと、攻撃そのものの受信を回避するための仕組みが重要となる。前者に関しては、正規のブロック取得をできる限り阻害せずに攻撃の早期検知を可能とするタイムアウト制御方式を検討する。後者に関しては、隣接ノードごとの過去の通信履歴を基に、将来の正常なブロック取得が期待できるノードの推定方式を検討する。

9．次年度使用が生じた理由と使用計画

(理由) 新型コロナウイルスの感染状況により国内外の学会が現地開催からオンライン開催に変更されるケースが多く発生したため、学会への参加費用に変更が生じたこと。また、導入を予定していた計算機の発売時期が遅れているため。

(使用計画) 学会の開催形態に関しては、今年度も引き続き新型コロナウイルスの感染状況により変化する可能性が高いため、状況の変化に注意し、対応する。また、導入を予定していた計算機は次年度中には発売される見通しのため、その際の購入費用の一部に充てる予定である。

10．研究発表（令和2年度の研究成果）

〔雑誌論文〕 計1件（うち査読付論文 1件／うち国際共著 0件／うちオープンアクセス 0件）

1．著者名 Sasabe Masahiro	4．巻 180
2．論文標題 Mathematical epidemiological analysis of dynamics of delay attacks on pull-based competitive information diffusion	5．発行年 2020年
3．雑誌名 Computer Networks	6．最初と最後の頁 107383:1～9
掲載論文のDOI（デジタルオブジェクト識別子） 10.1016/j.comnet.2020.107383	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0件

〔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

-