論文 / 著書情報
Article / Book Information

題目(和文)	
Title(English)	Primitives and Variants of the Proof-of-Work Mechanism in Blockchain-Based Consensus Protocols
著者(和文)	蘇翔宇
Author(English)	Xiangyu Su
出典(和文)	学位:博士(理学), 学位授与機関:東京工業大学, 報告番号:甲第12511号, 授与年月日:2023年9月22日, 学位の種別:課程博士, 審査員:田中 圭介,伊東 利哉,尾形 わかは,鹿島 亮,安永 憲司
Citation(English)	Degree:Doctor (Science), Conferring organization: Tokyo Institute of Technology, Report number:甲第12511号, Conferred date:2023/9/22, Degree Type:Course doctor, Examiner:,,,,
学位種別(和文)	博士論文
Category(English)	Doctoral Thesis
種別(和文)	審査の要旨
Type(English)	Exam Summary

（博士課程）

論文審査の要旨及び審査員

報告番号	甲第　　号		学位申請者氏名		蘇 翔宇	
論文審査 審査員		氏　名	職　名		氏　名	職　名
	主査	田中 圭介	教授	審査員	安永 憲司	准教授
	審査員	伊東 利哉	教授			
		尾形 わかは	教授			
		鹿島 亮	准教授			

論文審査の要旨（2000字程度）

本論文は、「Primitives and Variants of the Proof-of-Work Mechanism in Blockchain-Based Consensus Protocols（ブロックチェーンに基づく合意形成手法における Proof of Work メカニズムの構成要素とそのバリエーション）」と題し、英文全6章からなる。

合意形成は 50 年以上にわたる長年の研究テーマである。有名なビザンチンフォールトトレランスアルゴリズムや最近のブロックチェーン技術など、数多くの成果が提案されている。ブロックチェーンに基づく合意形成プロトコルは、従来のビザンチンフォールトトレランスアルゴリズムに比べて通信コストを削減することができるが、ブロックチェーンの中核、特にハッシュベースの Proof of Work (PoW) には現在莫大なエネルギーコストがかかっている。本論文では、より有意義なタスクに基づく PoW フレームワークを提案することを目的とする。

第1章「Introduction」では合意形成、ブロックチェーン、PoW メカニズムの背景を紹介する。現在一般的に採用されているハッシュベースの PoW 構造と、Proof of Stake や Proof of Useful Work などの既存の PoW のバリエーションの概要を述べる。加えて、ブロックチェーンプロトコルのセキュリティを維持しつつ、不必要なハッシュ計算をより有意義な計算によって置き換えることができることを指摘する。

第 2 章「Preliminaries」では、一般的なブロックチェーンモデルと安全性定義（すなわち、永続性と有効性）に対する定式化を行う。さらに、既存の PoW のバリエーションを一般的な Proof of X フレームワークに抽象化する。

第3章「Proof-of-Work Constructions from Computationally Hard Primitives」では、一方向性トラップドア関数と計算困難関数に基づく汎用的な PoW の構築を提案する。まず、計算困難関数に基づく PoW、および時間複雑さ、領域複雑さに依存する計算困難関数の定義を与える。つぎに、一方向性トラップドア関数を RSA 問題で具体的に構成する。さらに時間困難関数を RSW タイムロックパズルで、領域困難関数を DIODON 関数で具体的に構成し、これらの具体的構成が定義した安全性を満たすことを示す。これら具体的構成では既存方式が用いていたランダムオラクルモデルへの依存を取り除いている。

第4章「Provably Secure Blockchain Protocols from Distributed Proof-of-Deep-Learning」ではまず、深層学習を行う分散可能な Proof of Useful Work を提案し、これに基づくブロックチェーンプロトコルを設計する。このブロックチェーンプロトコルは、2 つの異なるチェーン選択ルール、すなわち最長チェーンルールと重みベースルールの下で、永続性と有効性に対する安全性を証明することができる。既存の深層学習を行う Proof of Useful Work と比較して、提案方式は強い仮定を用いない。また、参加者が他の参加者の事前に訓練されたモデルを用いることで、計算資源の浪費を軽減する。さらに、既存の深層学習ベースの Proof of Useful Work では達成されていなかった、ブロックチェーンプロトコルの安全性証明を与えている。

第 5 章「Blockchain Consensus from Score-Based Bid Assignment Problems」では、参加者が入札を行い、その入札がマッチングされて取引が成立する入札システムの概要についてまず述べる。つぎに、マッチングによる手法を入札割り当て問題と呼ぶ多対多の割り当て問題に抽象化する。さらに重みベースの PoW を一般的な Proof of X フレームワークに拡張する。本論文ではこのようなフレームワークの拡張を用いることでツリー構造に基づく新しい合意形成メカニズムを提案し、その安全性証明を与えている。

第6章「Conclusion and Future Work」では、本論文の結論を述べるとともに今後の課題について議論を行なっている。

以上のように、本論文は PoW メカニズムのバリエーションを考察し、証明可能で安全なブロックチェ

ーンベースの合意形成プロトコルを提案している。本論文は合意形成プロトコルに対して理論的、実用的な観点から新たな知見を与えるものであり、ブロックチェーン技術分野の発展に寄与し、理学上貢献するところ大である。よって， 本論文は博士(理学)の学位論文として十分価値があるものと認める。

注意：「論文審査の要旨及び審査員」は、東工大リサーチリポジトリ(T2R2)にてインターネット公表されますので、公表可能な範囲の内容で作成してください。