論文 / 著書情報
Article / Book Information

題目(和文)	
Title(English)	Lightweight Offchain Protocols for UtxO Based Ledgers
著者(和文)	JourenkoMaxim
Author(English)	Maxim Jourenko
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12061号, 授与年月日:2021年9月24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,首藤 一幸,森 立平
Citation(English)	Degree:Doctor (Science), Conferring organization: Tokyo Institute of Technology, Report number:甲第12061号, Conferred date:2021/9/24, 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

別　紙　1（論文博士）

論文審査の要旨及び審査員　（2000字程度）

報告番号	乙 第　　号	学位申請者	Maxim Jourenko	
論文審査員	氏　　名	職　　名	氏　　名	職　　名
	主査　田中圭介	教授	首藤一幸	准教授
	尾形わかは	教授	森立平	助教
	伊東利哉	教授		
	鹿島亮	准教授		

本論文は「Lightweight Offchain Protocols for UTxO Based Ledgers（UTxOをベースとして台帳に対する軽量のオフチェーンプロトコル）」と題し、英文で全6章から構成されている。

現在、ブロックチェーン技術の利用が高まり、ブロックチェーンベースのシステムのスケーラビリティの限界が浮き彫りになってきている。決済などの取引が台帳に記録されるためには、マイナーと呼ばれる多くの参加者によるコンセンサス・メカニズムによって処理される必要がある。しかしながら、システムのセキュリティを確保する目的などのため、一定時間にコンセンサス・メカニズムで処理できるトランザクションの数は限られている現状がある。

本論文では、このスケーラビリティの問題を解決するための一つの手段であるオフチェーンプロトコル（正規のプロトコルの外でも処理を行うプロトコル）を UTxO（Unspent Transaction Output、未使用トランザクション出力）をベースとした台帳に対して提案し、従来手法と比較してコストの少ない方式の提案に成功している。

第1章「Introduction」では、本論文の導入として、論文全体の概要について述べるとともに、本論文の背景となるブロックチェーンのスケーラビリティを解決するための一般的な考え方について解説している。ここでは特に、本論文の提案手法で対象とする、オフチェーンプロトコルやオフチェーンチャネルに対応するレイヤ2プロトコルに焦点を当てて説明を行なっている。

第2章「Background: Offchain Protocols」では、本論文の提案手法の対象であるオフチェーンプロトコルについて詳細に解説している。重要な概念である、対ごとのチャネルおよびチャネルの状態について説明を行なったのち、レイヤ2プロトコルに対する既存研究成果の分類手法を提案している。ここでは、オフチェーンチャネルに対するレベル、ネットワークに対するレベル、ネットワーク制御に対するレベルといったレベル分けを行うことで、詳細な分類を行うことを可能としている。

第3章「A Framework for UTxO Based Offchain Protocols」では、本研究の対象であるUTxOについて解説した後、UTxO下で動作するブロックチェーンに対してモデル定義を行なっている。トランザクション木と呼ばれる重要な概念についてもここで導入している。その上で、セキュリティモデルについて提案し、オフチェーンプロトコル構築のためのフレームワークを紹介している。

第4章「Lightweight Virtual Payment Channels」では、第3章で導入されたフレームワークを用いて具体的なプロトコルの提案を行なっている。ここでは、対ごとのペイメントチャネルが活用されており、Universal Composability（汎用結合可能性）という強力な安全性を証明するための枠組みの提供とその枠組みでの具体的な安全性証明も行われている。

第5章「Payment Trees」では、第3章で導入されたフレームワークを用いたふたつ目のプロトコルの手案を行なっている。このプロトコルはスマートコントラクトを必要とせず、ペイメントチャネルネットワーク内のパス間での支払いを可能にし、対数となるような個別の担保しか必要としない特徴をもっている。

第6章「Conclusion」では、本論文の総括と、今後の課題について述べている。

以上のように、本研究はブロックチェーンにおけるオフチェーンプロトコル技術に関して、プロトコル設計のフレームワーク、安全性証明の枠組み、具体的なプロトコルの提案、また提案プロトコルに対する安全性証明を与えるなど多くの知見を与えており、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。