T2R2 東京科学大学 リサーチリポジトリ
Science Tokyo Research Repository

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)	論文要旨
Type(English)	Summary

Powered by T2R2 (Science Tokyo Research Repository)

（論文博士）
(Dissertation Doctorate)

論　文　要　旨（英文）　（**800**語程度）

Dissertation Summary (approx. 800 words in English)

報告番号 For administrative use only	乙 第　　号	氏　名 Name	Jourenko Maxim

（要　旨）
(Summary)

Blockchain based decentralized ledgers as introduced by Nakamoto have enjoyed popularity and received interest from the research community and practitioners alike. Consensus protocols allow these ledgers to be operated by mutually distrustful parties at the cost of limited throughput. This limited throughput results in high fees that have to be paid by parties who intend to issue transactions. This is especially true in the case of high demand where, for instance, in December 2017 the average transaction fee in Bitcoin was above 50$. Moreover, the minimal confirmation time for a transaction on Bitcoin is 60 minutes.

There are two paradigms for the design of decentralized ledger. For one, there are ledgers based on Unspent Transaction Outputs (UTxO) as Bitcoin where UTxO represent the coins that are in circulation. Each UTxO contains a script specifying the coins owner. These coins can then be spent by transactions that consume existing UTxO and create new UTxO with potentially different ownership, thus performing payments. For another, there are ledgers based on accounts such as Ethereum where each entity is identified through an account and each account and all coins in circulation are distributed among accounts. In addition, smart-contracts are accounts that that are not controlled by any party but instead are linked to a program written in a Turing complete language that describes their behaviour.

The main motivation for the development of offchain protocols is to close the gap in transaction throughput to conventional systems like Visa. Offchain protocols operate on structures called offchain channels. Such channels are created between two parties and allow them to perform payments among each other without the need of interacting with the ledger. In contrast to payments on a ledger, these payments do not require any fees and are confirmed instantly. Channels can be concatenated into channel networks, offering a versatile and promising scalability solution.

There are multiple channel implementations that can be distinguished between payment channels and state channels. Existing payment channel implementations are designed for UTxO based ledger and due to their limitation only allow for payments. State channels make use of smart-contracts which

allows parties to execute state machines offchain. The expressiveness of state channels allows for creation of complex protocols such as virtual channels and efficient payments.

Our contributions to the field are as follows. (1) We formalize blockchains operating under the Unspent Transaction Output (UTxO) paradigm, as Bitcoin, and provide a framework for the creation of offchain protocols. Using this framework we (2) analyze the AMCU protocol, identify a vulnerability in it and present an attack on their security. (3) We create the Payment Trees protocol, a protocol for low collateral payments in offchain channel networks, making them resilient to Denial of Service attacks. (4) We create the lightweight virtual payment channels offchain protocol that allows to extend channel networks with virtual channels, and prove the protocol's security in the Universal Composability framework.

Our framework is based on the observation that, within the UTxO model, channels and their state are represented through a set of transactions that form directed acyclic graphs, i.e. trees. Our framework consists of three techniques that allow secure operations on such graphs of transactions thus altering the channel's state. (1) We can modify trees, (2) we can atomically construct sub-trees that have one common root, (3) we can atomically construct sub-trees that have two common roots. Here, atomically means that either all transactions within a sub-tree are created or none. While the first two techniques were implicitly used in previous work, the third technique is novel and it is what allows us to construct our protocols.

The Lightweight Virtual Payment channel protocol is performed on two adjacent channels, one between Alice and Bob and one between Bob and Charlie. We use the techniques within our framework to step-by-step modify both channels such that they are extended with a third channel, i.e. one between Alice and Charlie. This is done by bringing Bob into a position where they can enforce security of the construction, but are punished in the case they fail to do so. All while ensuring two properties (1) balance security, i.e. no honest party can lose coins, and (2) liveness, all of the coins are eventually accessible to the parties. This protocol is secure in the presence of a malicious adversary who can corrupt all but one parties and make them deviate from the protocol arbitrarily. Our construction can be used iteratively to construct virtual channels across multiple hops of an underlying channel network. The Payment Trees protocol is derived from the virtual channel protocol but optimized for efficient payments across payment channel networks.

In summary, our work improves the versatility of offchain channel networks, improving the state of the art, and closing the gap between constructions based on UTxO and constructions based on smart-contracts.

備考：論文要旨は、和文2000字と英文300語を1部ずつ提出するか、もしくは英文800語を1部提出してください。
Note: Dissertation summaries must be written in either of the following formats: (A) both in Japanese (approx. 2000 characters) and in English (approx. 300 words), or (B) in English (approx. 800 words).
注意：論文要旨は、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。

2013.8改訂
Revised August 2013

Important: Dissertation summaries will be published online on the Tokyo Tech Research Repository (T2R2). Do not include information treated as confidential under certain circumstances.