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)	論文要旨
Type(English)	Summary

（博士課程）
Doctoral Program

論 文 要 旨

THESIS SUMMARY

系・コース： Department of, Graduate major in	数理・計算科学 系 数理・計算科学 コース	申請学位（専攻分野）： Academic Degree Requested	博士 Doctor of （ 理学 ）
学生氏名： Student's Name	蘇 翔宇 (Xiangyu Su)	審査員主査： Chief Examiner	田中 圭介

要旨（英文 800 語程度）
Thesis Summary (approx.800 English Words)

Consensus has been a long-standing research topic in the field of distributed systems. Participants in a consensus protocol seek to agree on a log of messages that satisfies two crucial properties. (1) Persistence: all honest participants' logs agree with each other except for some logs may progress faster than others; (2) Liveness: messages received as input by honest participants get confirmed in all honest participants' logs quickly. Conventionally, this can be achieved by the Byzantine Fault-Tolerance algorithms. However, the high communication complexity of these algorithms prevents them from being deployed in large-scale networks, e.g., decentralized digital currency systems, in which consensus is necessary for settling transactions.

In light of early attempts of digital currencies, Satoshi Nakamoto proposed the Bitcoin system atop a proof-of-work (PoW)-based blockchain protocol. On a high level, a blockchain is formed by chaining blocks of messages (or transactions in the case of digital currency) with hash functions, i.e., by requiring the later block to include the hash of its previous block. In order to generate a block, the PoW mechanism requires its participants (usually called provers or miners) to solve a moderately hard computational task. Hence, provers who successfully solve the task are eligible to collect transactions and generate a block.

The public verifiability of the hash chain and the task guarantees that any participants in a blockchain protocol can verify the validity of any given block or blockchain. Moreover, due to the difficulty of PoW, the number of valid blocks generated during a time period is bounded by the provers' computing power. If the number is one, participants will agree on the only valid block to extend the blockchain. Otherwise, there will be ``forks''. By assuming the honest majority, i.e., more than half of the participants are honest, and applying concrete chain selection rules, e.g., the longest-chain rule or the weight-based blockchain framework, the shorter or lighter chain (fork) will eventually ``die out''. The reason is that honest computing power within the network will concentrate on the longest or the heaviest chain and outperform adversaries who intend to work on other forks.

Considering concrete PoW schemes, the most well-adopted construction is based on hash functions. Given a difficulty parameter T>0, provers are required to find a nonce such that the hash of the previous block and the nonce is less than T. For a hash function mapping strings of any arbitrary length to n, finding a valid nonce is expected to need 2^n/T hash evaluations. In contrast, the verification requires only one hash check.

Although it has been proven that the Nakamoto-style blockchain protocol from the aforementioned hash-based PoW satisfies persistence and liveness under the random oracle model, the hash evaluation itself is wasteful in energy and meaningless other than generating blocks. Therefore, numerous alternative PoW schemes have been proposed to utilize more ``useful'' tasks, e.g., proof-of-useful-work (PoUW), or other resources, e.g., proof-of-stake and proof-of-space.

This thesis will present three results related to these primitives and variants of PoW.

In the first result, we look back into the origin of PoW, which is a resource-demanding verifiable computation (for combating junk mail). Instead of hash functions, we show a generic construction based on one-way trapdoor functions and asymmetrically hard functions. The latter can be instantiated with primitives using different resources, e.g., time and memory. Hence, this approach enables us

to build time-hard and memory-hard PoW schemes.

Next, in terms of PoUW-based blockchain protocols, we investigate a subset of the PoUW, which takes deep learning tasks as useful work. We propose a distributed proof-of-deep-learning (D-PoDL) scheme and transform it into a blockchain protocol. The protocol is versatile enough to consider both the longest-chain rule and the weight-based blockchain framework. We are the first to prove persistence and liveness for blockchain protocols from deep learning-based PoUW schemes.

Finally, in the last result, we consider a competitive PoX framework in which difficulty is derived from the competition among provers instead of the underlying task. We abstract this framework from the bidding and matching operations in general double auction systems. The framework can also be regarded as an extension of the weight-based blockchain framework. In contrast to their restricted weight distribution, we show a consensus protocol design based on the competitive PoX that can achieve consensus on a blockchain assuming arbitrary score distribution.