1版

様　式　Ｃ－１９、Ｆ－１９－１、Ｚ－１９　（共通）

科研費
KAKENHI

科学研究費助成事業　　研究成果報告書

令和　４ 年　 ６ 月 ２８ 日現在

機関番号：２１６０２

研究種目：若手研究

研究期間：2019～2021

課題番号：１９Ｋ２０２５８

研究課題名（和文）Resilient Blockchain for Secure Information Sharing in Disaster Environment

研究課題名（英文）Resilient Blockchain for Secure Information Sharing in Disaster Environment

研究代表者

李　鵬（李鵬）（LI, Peng）

会津大学・コンピュータ理工学部・上級准教授

研究者番号：３０７３５９１５

交付決定額（研究期間全体）：（直接経費）　　3,000,000円

研究成果の概要（和文）：この研究の目的は、災害環境で安全な情報共有を行うためのブロックチェーンシステムを開発することである。 ブロックチェーンを用いて、低コスト、高セキュリティ、強力な柔軟性を備えた分散型情報共有を可能にすることを提案した。 災害環境の特別な課題に対処するために、復元力のあるコンセンサスプロトコルや軽量のブロックチェーンノードなど、多くの新機能を開発することで、既存のブロックチェーン技術をさらに強化した。 研究結果は、一流の国際ジャーナル（IEEETETCやIEEEJSACなど）や会議（IEEE INFOCOMなど）に掲載されている。

研究成果の学術的意義や社会的意義
ブロックチェーンを使用して、低コスト、高セキュリティ、強力な柔軟性を備えた分散型情報共有を可能にすることを提案します。 災害後、政府および非政府組織はこのシステムを使用して災害救援活動に協力することができます。

研究成果の概要（英文）：The goal of this research is to develop a resilient blockchain system for secure information sharing in disaster environment. We propose to use blockchain to enable decentralized information sharing with low-cost, high security and strong flexibility. To address special challenges of disaster environment, we further enhance existing blockchain techniques by developing many new features, e.g., resilient consensus protocols and light-weight blockchain nodes. The research results have been published in top international journals (e.g., IEEE TETC and IEEE JSAC) and conferences (e.g., IEEE INFOCOM).

研究分野：情報ネットワーク

キーワード：ブロックチェーン

１．研究開始当初の背景

After big disasters (e.g., earthquake), governmental and non-governmental organizations quickly react to join disaster relief activities. Instead of working independently, these organizations collaborate on recovery operations, medical support and distribution of food and water. For example, an earthquake struck Kumamoto in 2016. The local government, fire stations, hospitals, transportation and international organizations provided various disaster relief (https://en.wikipedia.org/wiki/2016_Kumamoto_earthquakes). Therefore, there are high demands of building an information sharing system to enable their collaboration.

Existing works for information sharing after disaster. In the past a few years, many research has studied information sharing after disaster. For example, Movable and Deployable Resource Units (MDRUs) have been developed to providing communication services in disaster-stricken area [Kato et al. IEEE Network, 2016]. MDRUs can be carried by vehicles and they contain computing and network devices. Based on MDRUs, our research team has developed an information management system, called RIM, which enables information sharing among different organizations [Li et al., IEEE Trans. Emerg. Topics Comput., 2017]. However, all existing systems use centralized or distributed databases, which faces several critical challenges: (a) Storing all data at a centralized database is unsafe. The servers installing the database may stop working due to power shortage. (b) Although distributed databases have no single-point failure problem, but its robustness and flexibility are poor. Organizations may join or leave the system at any time. It is difficult to reconfigure the databases in such a dynamic environment. (c) Database systems have serious security and privacy problem. In disaster, organizations may share some sensitive data (e.g., data from hospitals and insurance companies) that contains many private contents. On the other hand, we do not have sufficient hardware and software resources to protect the shared data in disaster environment. The data can be easily stolen or deleted from databases if attackers hack into the system.

２．研究の目的

The main purpose of this research is to develop a resilient blockchain for secure information sharing in disaster management. An overview is shown in Figure 1. There could be multiple permissioned chains ("permissioned" means organizations need to have certificates to join). An organization can join multiple chains at the same time. Once an organization joins a chain, it can read/write data from/to the chain under the consensus protocol. Different chains can share data via our developed side chain technique. Disaster environment is very special, where IT infrastructure (e.g., servers and network switches) could be damaged or cannot fully work due to power shortage. Our experiences show that all traditional database work poorly in disaster environment. Our proposed blockchain is promising in addressing data sharing challenges in disaster. It has advantages of data transparency, enhanced security, improved traceability and low cost.

３．研究の方法

To achieve our research goals, we have studied the following three research tasks.

A. Build a basic blockchain system that is tailored for disaster environment

We build a basic blockchain system, whose blocks are used for storing structured and unstructured data. It also has modules of network management and authentication control. Applications invoke smart contracts to access blockchains. We abstract typical application operations and create smart contract templates, so that users can quickly find smart contracts that satisfy their requirements. (3) Quick deployment: existing permissioned blockchain systems (e.g., Hyperledger Fabric) need complex configurations (i.e., write many scripts and manually configure network). We will develop a set of automatic configuration tools, to simply the deployment of the blockchain system. By using our tools, people without strong ICT skills (e.g., doctors and firemen) can quickly use their own servers to join our blockchain network.

B. Consensus protocol optimization

Consensus protocol is the core of blockchain, but face new challenges in disaster. Permissioned organizations can join and leave the blockchain at any time. Further, network conditions change rapidly, leading to message loss. Sharding can significantly improve the blockchain scalability, by dividing nodes into small groups called shards that can handle transactions in parallel. However, all existing sharding systems adopt complete sharding, i.e., shards are isolated. It raises additional overhead to guarantee the atomicity and consistency of cross-shard transactions and seriously degrades the sharding performance. In this paper, we present Pyramid, the first layered sharding blockchain system, in which some shards can store the full records of multiple shards thus the cross-shard transactions can be processed and validated in these shards internally. When committing cross-shard transactions, to achieve consistency among the related shards, a layered sharding consensus based on the collaboration among several shards is presented. Compared with complete sharding in which each cross-shard transaction is split into multiple sub-transactions and cost multiple consensus rounds to commit, the layered sharding consensus can commit cross-shard transactions in one round. Furthermore, the security, scalability, and performance of layered sharding with different sharding structures are theoretically analyzed. Finally, we implement a prototype for Pyramid and its evaluation results illustrate that compared with the state-of-the-art complete sharding systems, Pyramid can improve the transaction throughput by 2.95 times in a system with 17 shards and 3500 nodes.

C. Improvement of system scalability
Off-blockchain payment channels can significantly improve blockchain scalability by enabling a large number of micro-payments between two blockchain nodes, without committing every single payment to the blockchain. Multiple payment channels form a payment network, so that two nodes without direct channel connection can still make payments. A critical challenge in payment network construction is to decide how many funds should be deposited into payment channels as initial balances, which seriously influences the performance of payment networks, but has been seldom studied by existing work. In this paper, we address this challenge by designing PnP, a balance planning service for payment networks. Given estimated payment demands among nodes, PnP can decide channel balances to satisfy these demands with a high probability. It does not rely on any trusted third-parties, and can provide strong protection from malicious attacks with low overhead. It obtains these benefits with two novel designs, the cryptographic sortition and the chance-constrained balance planning algorithm. Experimental results on a testbed of 30 nodes show that PnP can enable 30% more payments than other designs.

４．研究成果

[1]. X. Luo and Peng Li, “Learning-Based Off-Chain Transaction Scheduling in Prioritized Payment Channel Networks”, IEEE Journal on Selected Areas in Communications, accepted.

[2]. X. Liu, Z. Tang, Peng Li, S. Guo, X. Fan and J. Zhang, "A Graph Learning Based Approach for Identity Inference in DApp Platform Blockchain," in IEEE Transactions on Emerging Topics in Computing, vol. 10, no. 1, pp. 438-449, 1 Jan.-March 2022, doi: 10.1109/TETC.2020.3027309.

[3]. Z. Hong, S. Guo, Peng Li and W. Chen, “Pyramid: A Layered Sharding Blockchain System”, IEEE INFOCOM 2021.

[4]. Peng Li, Toshiaki Miyazaki, and Wanlei Zhou, “Secure Balance Planning of Off-blockchain Payment Channel Networks”, IEEE INFOCOM 2020.

[5]. Z. Hong, S. Guo, R. Zhang, Peng Li, Y. Zhan and W. Chen, "CYCLE: Sustainable Off-Chain Payment Channel Network with Asynchronous Rebalancing", IEEE/IFIP International Conference on Dependable Systems and Networks (DSN), 2022

５．主な発表論文等

〔雑誌論文〕　計3件（うち査読付論文　2件／うち国際共著　2件／うちオープンアクセス　0件）

１．著者名 Xiaoping Zhou, Peng Li, Toshiaki Miyazaki and Peng Liu	４．巻 E104-D
２．論文標題 A Fast Algorithm for Liquid Voting on Blockchain	５．発行年 2021年
３．雑誌名 IEICE Transactions on Communications	６．最初と最後の頁 1001-1010
掲載論文のDOI（デジタルオブジェクト識別子） なし	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 該当する

１．著者名 Yufeng Zhan, Song Guo, Peng Li and Jiang Zhang	４．巻 69
２．論文標題 A Deep Reinforcement Learning based Offloading Game in Edge Computing	５．発行年 2020年
３．雑誌名 IEEE Transactions on Computers	６．最初と最後の頁 883-893
掲載論文のDOI（デジタルオブジェクト識別子） 10.1109/TC.2020.2969148	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 該当する

１．著者名 Liu Xiao、Tang Zaiyang、Li Peng、Guo Song、Fan Xuepeng、Zhang Jinbo	４．巻 10
２．論文標題 A Graph Learning Based Approach for Identity Inference in DApp Platform Blockchain	５．発行年 2022年
３．雑誌名 IEEE Transactions on Emerging Topics in Computing	６．最初と最後の頁 438～449
掲載論文のDOI（デジタルオブジェクト識別子） 10.1109/TETC.2020.3027309	査読の有無 無
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4件（うち招待講演　0件／うち国際学会　4件）

１．発表者名 Zicong Hong, Song Guo, Peng Li and Wuhui Chen
２．発表標題 Pyramid: A Layered Sharding Blockchain System
３．学会等名 IEEE International Conference on Computer Communications (INFOCOM)（国際学会）
４．発表年 2021年

１．発表者名
Peng Li, Toshiaki Miyazaki, and Wanlei Zhou

２．発表標題
Secure Balance Planning of Off-blockchain Payment Channel Networks

３．学会等名
IEEE International Conference on Computer Communications (INFOCOM)（国際学会）

４．発表年
2020年

１．発表者名
Peng Li, Xiaofei Luo, Toshiaki Miyazaki, and Song Guo

２．発表標題
Privacy-preserving Payment Channel Networks using Trusted Execution Environment

３．学会等名
IEEE International Conference on Communications (ICC)（国際学会）

４．発表年
2020年

１．発表者名
Z. Hong, S. Guo, R. Zhang, Peng Li, Y. Zhan and W. Chen

２．発表標題
CYCLE: Sustainable Off-Chain Payment Channel Network with Asynchronous Rebalancing

３．学会等名
IEEE/IFIP International Conference on Dependable Systems and Networks (DSN)（国際学会）

４．発表年
2022年

〔図書〕　計0件

〔産業財産権〕

〔その他〕

－

６．研究組織

	氏名 （ローマ字氏名） （研究者番号）	所属研究機関・部局・職 （機関番号）	備考

７．科研費を使用して開催した国際研究集会

〔国際研究集会〕　計0件

８．本研究に関連して実施した国際共同研究の実施状況

共同研究相手国	相手方研究機関