











Multi-ledger Coordinating Mechanism by Smart Contract for Individual-Initiated Trustworthy Data Sharing

Yenjou Wang¹ , Ruichen Cong¹ , Yixiao Liu¹ , Kiichi Tago² , Ruidong Li³ ,
Hitoshi Asaeda⁴ , and Qun Jin⁵  

¹ Graduate School of Human Sciences, Waseda University, Tokorozawa, Japan

² Department of Information and Network Science, Chiba Institute of Technology, Narashino, Japan

³ Faculty of Electrical, Information and Communication Engineering, Institute of Science and Engineering, Kanazawa University, Kanazawa, Japan

⁴ National Institute of Information and Communications Technology (NICT), Tokyo, Japan

⁵ Faculty of Human Sciences, Waseda University, Tokorozawa, Japan

jin@waseda.jp

Abstract. With the development of the Internet of Things (IoT) and sensors, personal health data can be collected by wearable devices. However, one of the biggest concerns about the storage and use of sensitive personal health data is privacy. To address this issue, we propose a new Multi-Ledger Coordinating Mechanism (MLCM) with blockchain for trustworthy data sharing under the control of each individual data owner. MLCM, enabled by smart contracts, lets an individual user control and manage all his/her own data in a flexible way and enhances data security and privacy preservation in user authentication and management. Also, all activities related to data access are monitored and further recorded in blockchain. The evaluation experiment is designed to demonstrate the feasibility of the proposed mechanism, and the result shows that the prototype implementation of one smart contract based on Hyperledger Fabric is stable.

Keywords: Blockchain · IPFS · Smart Contract · Privacy Protection · Data Sharing · Personal Health Data

1 Introduction

With the rapid development of Internet of Things (IoT) technology, sensors make it possible to collect a large amount of data for higher levels of services through data sharing, such as personalized healthcare services. In particular, the health data collected for a person by wearable devices is called Personal Health Data (PHD), which may include privacy. Privacy protection is a complex and sensitive issue, which is a big challenge for data sharing [1]. Therefore, many countries have enacted laws to address privacy concerns. On the other hand, two complex issues should be considered, which are “who owns the data” and “what rights does ownership imply” [2]. For example,

medical service providers, such as hospitals, create medical records about patients as the data owner, but do not allow data sharing with patients. However, medical records are more related to patients in essence, and they should also be the data owner to control, manage and decide who can share and use the data. Therefore, practical solutions are necessary to secure personal data sharing and ensure individuals' data ownership.

In recent years, blockchain with decentralization and immutability has been used to be a helpful solution for implementing data privacy protection and secure data transmission. As mentioned above, PHD involves privacy and is sensitive, therefore, they are unsuitable for recording on blockchain in plaintext. An Individual-Initiated Auditable Access Control (IIAAC) mechanism was proposed in [3], which is based on a consortium blockchain, CP-ABE (Ciphertext-Policy Attribute-Based Encryption) and IPFS (InterPlanetary File System) to share encrypted PHD and enable data owners to define the access policy on their data initiatively.

Currently, many studies focus on using smart contracts or traditional access mechanisms to define access permissions [4, 5]. These authentication methods are preset when a user accesses blockchain for the first time, and the authentication data is recorded on the CA (Certificate Authority) or cloud server [6]. Since we target to provide an individual-initiated system for health and medical data sharing, it is necessary to consider the third-party certificates that can be used to authenticate the identity of different hospitals or different types of users. There must be a trusted manager as the authenticator to avoid identity forgery in each node when the users first register. We design a mechanism based on blockchain, in which the certification information and access logs are recorded to allow secure data sharing between hospitals and individual users and ensure that the information cannot be tampered with. In addition, recorded access logs on blockchain can also be used for subsequent discriminant analysis of illegal accesses.

To share PHD securely, this study proposes a Multi-Ledger Coordinating Mechanism (MLCM) for individual-initiated trustworthy data sharing enabled by smart contracts. Smart contracts are taken as the coordinator of ledgers, defining which actions can be performed by different types of users on which ledgers through MLCM. In MLCM, the access policy of personal data can be set by individuals flexibly, and the ownership of their data can be kept to individuals by smart contracts, even if others create the data. In addition, user authentication information can also be recorded and shared safely through smart contracts. Then MLCM, with the blockchain as a surveillance zone, is used to automatically record the access log to prevent not-targeted users from tampering with it for subsequent analysis. The major contributions of this study are summarized as follows.

- An individual-initiated system for health and medical data sharing based on blockchain ensures the ownership of data to individuals who can manage all their own data in a flexible way and enhances privacy protection.
- The multi-ledger coordinating mechanism allows different types of users to access different related ledgers, and to share and use data securely.
- The recordability of access enables illegal access to be monitored and analyzed.

The rest of this paper is organized as follows. In Sect. 2, we overview related work on data sharing and access control based on smart contracts. In Sect. 3, how to coordinate each ledger through smart contracts is explained in detail. In Sect. 4, we describe the

experiment environment for performance evaluation and discuss the results to demonstrate the feasibility and stability of the proposed mechanism. Finally, Sect. 5 concludes this work and highlights future directions.

2 Related Work

This section describes data sharing and access control by smart contracts based on blockchain platforms. A smart contract is a program that can be executed automatically after certain conditions are satisfied. It was initially introduced by Nick Szabo [7]. It can receive, store, send messages, and perform operations with predetermined rules. In addition, the integration of smart contracts and IoT with significant benefits are discussed, such as transaction management, distributed computing, data traceability, access control, etc. [8].

To enable secure sharing of sensitive data, such as PHD, many frameworks and approaches using smart contracts in blockchain have been proposed [9–13]. In previous studies, smart contracts have been used to achieve access control of medical data by using policies to remain patient centricity across the system. Saini et al. [9] developed an access control model based on smart contracts for smart healthcare services to secure sharing of electronic medical records (EMRs). The EMRs are encrypted and stored in the cloud, while the hash-values corresponding to the EMRs are stored on blockchain. However, the integration of blockchain and cloud incurs challenges of security, scalability, and performance, in which the attack and latency may occur in the centralized-cloud server. Putra et al. [10] use the Ethereum smart contract and re-encryption method to provide a safe electronic medical record data sharing method between hospitals and provide a reward mechanism to encourage data sharing. However, patients have no control over their PHD. Kumar and Dakshayini [11] proposed secure sharing of health data using Hyper ledger Fabric, a consortium blockchain platform, among medical organizations. However, there is a limitation on on-chain storage, which is the inefficiency of storing large size of data on blockchain.

Besides the utilization in access control, smart contracts are also used to register staff members of medical institutions before they request access to patients' electronic health records. Zaghoul et al. [12] proposed a security and privacy enhanced medical record sharing and management scheme. Two smart contracts are deployed for staff member registration (SMR) and access verification and permission announcements (AVPA). After verifying the attributes of staff members, which are physically certified by a registering institution first, the transaction between the SMR contract and the registering institution is executed. The attributes of staff members are stored on blockchain. In addition, patients can develop and deploy the AVPA contract to define who can obtain the electronic health record through blockchain initiatively. However, since user registration and access verification are performed by smart contracts, and the attributes data are stored in the smart contracts, it is necessary to optimize on-chain storage to improve the overall performance.

This study focuses on a new multi-ledger coordinating mechanism (MLCM), in which we design four ledgers as multi-ledger to let individuals manage their own data initiatively and further design three smart contracts for multi-ledger coordination. In our

proposed mechanism, different types of users are permitted to access different ledgers, and all access activities on blockchain are monitored and recorded.

3 Coordinating Multi-ledger by Smart Contracts

In this section, we first introduce the system architecture, which combines multi-ledger in blockchain, IPFS, and a client application that connects blockchain and IPFS. Then, we describe four ledgers in the system in terms of functions and their relationships with each other. Finally, we describe how the ledgers coordinate with each other through smart contracts and explain the detailed procedures in the system.

Trustworthy Data Sharing with Multi-ledger Coordinating Mechanism. To achieve trustworthy data sharing, a multi-ledger coordinating mechanism is proposed, which coordinates four ledgers to record users' PHD, electronic medical records, access logs and authentication data through three smart contracts. In this system, users are classified into three types: a general user (patient) who creates the PHD, the medical staff (doctor) who creates the electronic medical records, and the manager who perform user authentication and management. In this study, we focus on defining and constructing smart contracts for data sharing and access monitoring. CP-ABE, an attribute-based encryption scheme, lets users customize and manage the accessor attributes of their PHD reliably and flexibly. The system architecture is shown in Fig. 1, which mainly consists of four components: consortium blockchain, off-chain storage (IPFS), CP-ABE encryption mechanism, and a client application that connects blockchain and IPFS.

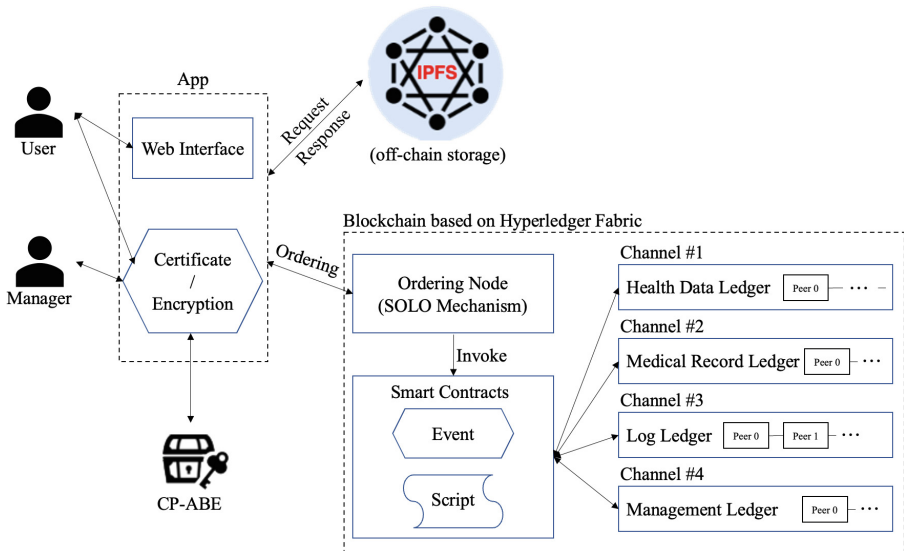


Fig. 1. System architecture

Multi-ledger for Encrypted Multi-Source Data. In this study, the users in the blockchain vary in attributes and organization, resulting in inconsistent content and

purpose for the stored data. Dividing the blockchain into multiple ledgers according to storage content and purpose can increase the efficiency of data sharing and access. Therefore, we design four ledgers for individual-initiated trustworthy data sharing. The membership service provider (MSP) is used to set the access permission for different user types on each ledger as shown in Table 1. The general user (patient) who owns the health data collected by wearable devices can read and write on the health data ledger. They can also have ownership to read their electronic medical records created by a medical staff through smart contracts. In the same way, the medical staff (doctor) who generates the electronic medical records can read and write on the medical record ledger and read permitted data in the health data ledger. General users and medical staffs have no permission to access the management ledger. In contrast, the manager has no permission to access the health data ledger and medical record ledger. However, the manager can read and write on the management ledger to record the authentication data. Furthermore, all blockchain users have read right on the log ledger to check if there is illegal access by malicious users. The data structure of each ledger is represented in JSON and is described as follows.

Table 1. Access permissions for different user types on each ledger by MSP

	General User (Patient)	Medical Staff (Doctor)	Manager
Health Data Ledger	Read/Write	Read Permitted Data Only	–
Medical Record Ledger	Read Owned Data Only	Read/Write	–
Log Ledger	Read Only	Read Only	Read Only
Management Ledger	–	–	Read/Write

Data Structure of Health Data Ledger. The hash values corresponding to the health data generated by wearable devices or other sensors and stored in IPFS are recorded in the health data ledger. As shown in Fig. 2, the data owner in the health data ledger records the user’s GID, which CP-ABE sets. Furthermore, the action in which reading or writing and timestamp in which the hash value is stored in the blockchain are recorded. In addition, to ensure the correlation between data, the hash value of data before being updated is also recorded if the data needs to be updated.

Data Structure of Medical Record Ledger. In the medical record ledger, the electronic medical records of patients created by the medical staff are recorded. As shown in Fig. 3, the medical staff (doctor)’s GID is registered as the data owner in the medical record ledger. Furthermore, to make a general user (patient) own his/her data, a smart contract is created for doubling ownerships (SCDO), which sets the doctor and patient as co-owner of the electronic medical records and the ownership information is stored in the medical record ledger.

Data Structure of Log Ledger. In the log ledger, for traceability on the blockchain, a smart contract monitors the blockchain and records all access events, actions, and reasons

```

{"healthdata_ledger":{
  "key": {
    "data_owner": GID_User,
  }
  "value" {
    "operation": {
      "action": "read"/"created"...
    },
    "hash": "jei273891wheu...",
    "prv_hash": "jeiqwejiq280391ejiqu...", "none",      # if update/revised
    "timestamp": 3728042
  }
}}

```

Fig. 2. Data structure of health data ledger

```

{"medicalrecord_ledger":{
  "key": {
    "data_owner": GID_Doctor, GID_USER,
  }
  "value" {
    "operation": {
      "action": "read"/"created"...
    },
    "hash": "jei273qejudiaseu...",
    "prv_hash": "jeiqwejiq280391ejiqu...", "none",      # if update/revised
    "creator": GID_Doctor/ GID_Nurse/ GID_Officer,
    "timestamp": 3728042
  }
}}

```

Fig. 3. Data structure of medical record ledger

to the log ledger. As shown in Fig. 4, the GID of the data owner and requestor, and the smart contract, which is used to execute the request, and the access token are recorded. In addition, the ID of the target data on IPFS, the hash value of target data returned from IPFS, and the metadata corresponding to the target data are also recorded in the log ledger. These data can be used for future analysis of user behaviors to detect illegal access.

Data Structure of Management Ledger. In the management ledger, the authentication data of the users' identities are recorded. Hyperledger Fabric, a consortium blockchain that allows one manager in each organization in the blockchain network, is used in the system. The manager is responsible for the initial identity authentication of the blockchain node. The authentication data on blockchain are shared through the management ledger to improve the efficiency of initial authentication. Since authentication is related to the security of the blockchain network, the management ledger can only be accessed by the manager as shown in Fig. 5, and the GID of the user, the action in which

```

{"log_ledger":{
  "value" {
    "data_owner": GID_USER/GID_Doctor/ GID_Supervisor,
    "controller": GID_SC,          #smartcontract's GID
    "creator": GID_USER/ GID_Doctor/ GID_Supervisor
    "access_token": "qwjieo23jlloeqw",
    "access_number": 123456,
    "status": "approved"/"rejected",
    "Target_hash": "jei27389qwereu...",
    "dataID_number": "123489",      #Data ID on IPFS
    "index":"heartbeat, weight, CA...", #keywords
    "operation":"read","created"....,
    "reason": "Daily upload"/"Medical records"/
              "Required for diagnosis and treatment"/"Authorize"....,
    "timestamp": 3728042
  }
}}

```

Fig. 4. Data structure of log ledger

reading or writing, and the CA name which authenticates the identity of the target user are recorded.

```

{"management_ledger":{
  "key": {
    "target_user": GID_USER,      #data_owner/CA authorized target
    "creator": GID_Supervisor    #CA's GID
  }
  "value" {
    "operation":{
      "action": "authorize","read"
    },
    "CA_name":"A hospital"/"B hospital"/"Root CA", #Where did user get the CA
    "number":234567,
    "access_transaction_no": 123456, #log_ledger_access_number
    "timestamp": 3728042
  }
}}

```

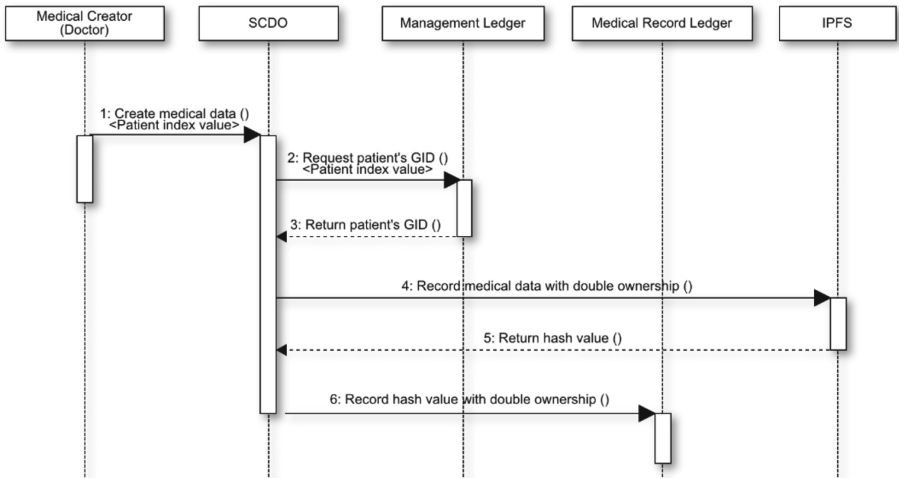
Fig. 5. Data structure of management ledger

Smart Contracts for Multi-ledger Coordination. To enhance the protection of privacy and data security, MLCM is proposed and designed, and it is enabled by smart contracts, namely smart contracts for doubling ownerships (SCDO), smart contracts for managing users (SCMU), and smart contracts for monitoring accesses (SCMA). The relationship between smart contracts and ledgers is shown in Table 2, and the detailed functions of each smart contract are described as follows.

Table 2. Multi-ledger coordination by smart contracts

	Smart Contracts for Doubling Ownerships (SCDO)	Smart Contracts for Managing Users (SCMU)	Smart Contracts for Monitoring Accesses (SCMA)
Health Data Ledger		✓	✓
Medical Record Ledger	✓	✓	✓
Log Ledger	✓	✓	✓
Management Ledger	✓	✓	✓

Smart Contracts for Doubling Ownerships (SCDO). To ensure the patients to have their own medical data ownership, SCDO is responsible for coordinating the medical records ledger, management ledger, and log ledger to let a specified medical record be owned by both the creator (doctor) and the patient. The process sequence of SCDO is shown in Fig. 6.

**Fig. 6.** The process sequence of smart contract for doubling ownerships (SCDO)

When the doctor generates a medical record for a patient, the SCDO requests the patient's GID from the management ledger based on the patient information provided

by the doctor and records the GID to the medical data. Medical record data with double-owners is recorded in IPFS. When the SCDO receives the hash value returned by IPFS, it creates a new transaction that records the double-owners' GIDs and hash value.

Smart Contracts for Managing Users (SCMU). To allow that the user's authentication data can be recorded in a private way and resolve the issue of repeated authentication. The manager records and shares the user's authentication with other nodes through SCMU. The process sequence of SCMU is shown in Fig. 7.

In SCMU, the authentication process is divided into two cases. (1) a new user has never registered in blockchain before, and (2) a user was authenticated in other nodes (e.g., hospitals). When the manager confirms that the authentication case is (1) from SCMU, the user needs to provide GID and attributes to the manager for authentication by the CP-ABE server. The authentication data is recorded to IPFS through SCMU. SCMU also sets the visitor list in the corresponding ledger through the user's attribute to ensure the user to access different ledgers which match his/her attributes. Finally, SCMU records the hash value returned by IPFS in the management ledger and notifies the manager that the identity authentication was succeeded.

When the manager confirms that the user authentication case is (2) from the management ledger, SCMU can send an authentication request to the previous authentication node (manager of the old node) through the information on the management ledger record. SCMU records the information of a new authorization node (manager of the new node) to IPFS, so that the manager of a new node can access the authentication data. Next, SCMU sends the authorization success message to the manager of the old node and the manager of a new node. Finally, the manager of a new node requests the authentication information from IPFS to complete the authentication process.

Smart Contract for Monitoring Accesses (SCMA). To enable all data to be shared trustworthily, SCMA is used to monitor and record all the access logs in blockchain. SCMA coordinates and monitors the health data ledger, medical record ledger, management ledger, and log ledger. These ledgers are represented as "Ledger" in Fig. 8. Through SCMA, all blockchain users' access activities are monitored and recorded to log ledger, e.g., a user uploads a new PHD, or a doctor views a case profile, etc. The process sequence of SCMA is shown in Fig. 8.

4 Experiment Result

To verify MLCM proposed in this study, we constructed a prototype of SCDO. We ran a workstation with Ubuntu 20.04, 48 logical CPUs, 140 GB main memory and 1TB storage capacity, and built the experiment environment based on Hyperledger Fabric 1.4.4. We used the docker version 20.10.12. The Go version is 1.13.8 Linux/amd64, and the tool for evaluating performance is Tape, which is a lightweight tool that can be used to measure TPS (Transactions Per Second) on Hyperledger Fabric.

In our experiment, we mainly evaluate the stability of smart contracts based on blockchain. Therefore, we replaced the hash value and other information returned by off-chain storage (IPFS) or application out of blockchain into a fixed string. The experiment is conducted with two actions, write, and read. Write is that the doctor creates the electronic

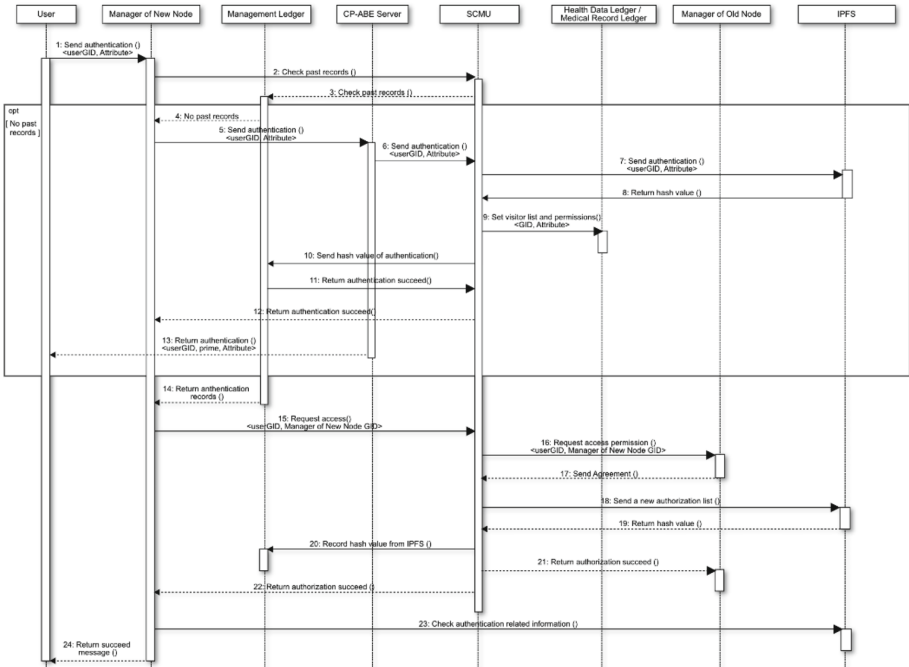


Fig. 7. The process sequence of smart contract for managing users (SCMU)

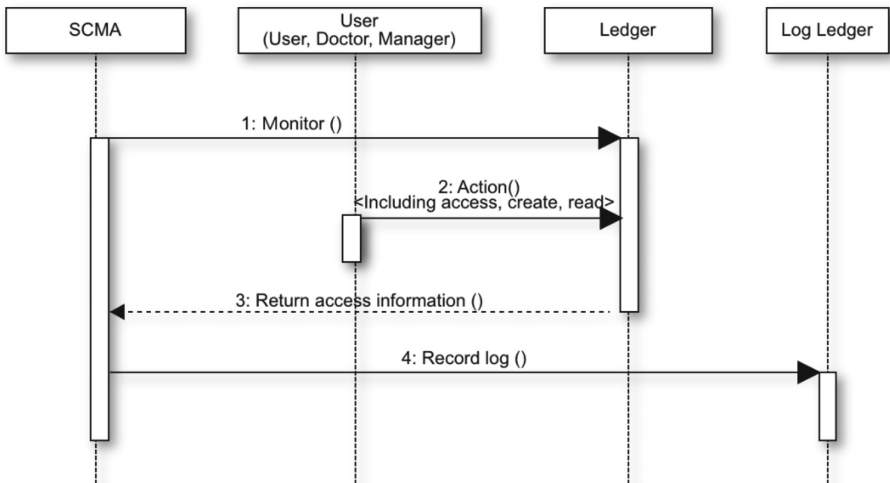


Fig. 8. The process sequence of smart contract for monitoring accesses (SCMA)

medical records, and then SCDO is used to copy the electronic medical records to create a transaction that includes the patient’s GID. Read fetches the medical records containing the patient’s GID and doctor’s GID and records the result to the log ledger by SCDO.

Tape is used to measure the duration, block number, and TPS for writing and reading data with SCDO. We carried out 200, 1000, and 10000 transactions to measure the throughput of the network traffic for reading and writing respectively. The results are shown in Table 3. In addition, duration is the execution time of all transactions, while blocks represent the number of blocks generated by the transaction. The results showed that all transactions were approved and recorded onto the blockchain with TPS staying steady at approximately 30, demonstrating that the SCDO architecture proposed in this study maintains availability and stability despite fluctuations in transaction volume.

Table 3. Transactions per second for smart contract for doubling ownerships (SCDO)

Transaction (time)	Action	Duration (second)	Blocks	TPS
200	Write	6.8	20	29.3
200	Read	6.8	20	29.1
1000	Write	31.1	100	32.1
1000	Read	33.2	100	30.1
10000	Write	325.2	1000	30.7
10000	Read	338.1	1000	29.6

5 Conclusion

In this study, we proposed a new Multi-Ledger Coordinating Mechanism (MLCM) based on blockchain that enables individual-initiated trustworthy data sharing under the control of the data owner. The proposed new mechanism can be expected to enhance the privacy preservation of personal health data in sharing and using. In this paper, we described how MLCM coordinates through three smart contracts. Under the MLCM architecture, all accesses are monitored. Users are more flexible and secure in defining their data access rights. The medical records created by the doctor can be shared with the patient by smart contracts for doubling ownership. In addition, all authentication information is recorded by a management ledger to ensure trustworthy data sharing. With sharing of data between hospitals, users already in the blockchain do not need to spend the time of re-authentication when entering a new node (hospital). We built a prototype of SCDO as the experiment environment based on Hyperledger Fabric. Through measuring the duration, block number, and TPS for writing and reading data with SCDO by Tape to evaluate the stability of MLCM. The result showed that the prototyping implementation based on Hyperledger Fabric is stable.

In future works, we plan to investigate illegal access on a blockchain and improve the access control mechanism through feature analysis utilizing machine learning techniques, aiming to effectively resolve the problem of consortium blockchain attacks initiated by malicious users.

Acknowledgement. The work was supported in part by 2020–2021 Waseda University-NICT Matching Funds Program, 2020–2025 JSPS A3 Foresight Program (Grant No. JPJSA3F20200001), 2022 Waseda University Grants for Special Research Projects (Nos. 2022C-225 and 2022R-036), 2022–2024 Masaru Ibuka Foundation Research Project on Oriental Medicine, 2022 JST SPRING (Grant No. JPMJSP2128), and 2022 Waseda University Advanced Research Center for Human Sciences Project (Grant No. BA080Z000300).

References

1. Data Revolution Group: A World that counts. <https://www.undatarevolution.org/report/>. Accessed 05 Feb 2023
2. Wry, T., Cobb, J.A., Aldrich, H.E.: Personal data: The emergence of a new asset class. World Economic Forum, Swiss (2011)
3. Cong, R., Liu, Y., Tago, K., Li, R., Asaeda H., Jin, Q.: Individual-initiated auditable access control for privacy-preserved IoT data sharing with blockchain. In: 2021 IEEE International Conference on Communications Workshops (ICC Workshops), Montreal, QC, Canada, pp. 1–6. IEEE (2021)
4. Griggs, K.N., Ossipova, O., Kohlios, C.P., Baccarini, A.N., Howson, E.A., Hayajneh, T.: Healthcare blockchain system using smart contracts for secure automated remote patient monitoring. *J. Med. Syst.* **42**(7), 1–7 (2018)
5. Zhang, X., Chen, X.: Data security sharing and storage based on a consortium blockchain in a vehicular ad-hoc network. *IEEE Access* **7**, 58241–58254 (2019)
6. Ur Rahman, M., Baiardi, F., Ricci, L.: Blockchain smart contracts for scalable data sharing in IoT: a case study of smart agriculture. In: 2020 IEEE Global Conference on Artificial Intelligence and Internet of Things (GCAIoT), Dubai, United Arab Emirates, pp. 1–7. IEEE (2020)
7. Szabo, N.: Formalizing and securing relationships on public networks. *First Monday* **2**(9) (1997). <https://doi.org/10.5210/fm.v2i9.548>
8. Peng, K., Li, M., Huang, H., Wang, C., Wan, S., Choo, K.-K.R.: Security challenges and opportunities for smart contracts in internet of things: a survey. *IEEE Internet Things J.* **8**(15), 12004–12020 (2021)
9. Saini, A., Zhu, Q., Singh, N., Xiang, Y., Gao, L., Zhang, Y.: A smart-contract-based access control framework for cloud smart healthcare system. *IEEE Internet Things J.* **8**(7), 5914–5925 (2021)
10. Putra, F.A., Febriansyah, H., Sari, R.F.: Blockchain-based data owner rating in medical record data sharing using ethereum. In: 2022 20th International Conference on ICT and Knowledge Engineering (ICT&KE), Bangkok, Thailand, pp. 1–9. IEEE (2022)
11. Kumar S.N., Dakshayini, M.: Secure sharing of health data using hyperledger fabric based on blockchain technology. In: 2020 International Conference on Mainstreaming Block Chain Implementation (ICOMBI), Bengaluru, India, pp. 1–5. IEEE (2020)
12. Zaghoul, E., Li T., Ren, J.: Security and privacy of electronic health records: decentralized and hierarchical data sharing using smart contracts. In: 2019 International Conference on Computing, Networking and Communications (ICNC), Honolulu, HI, USA, pp. 375–379. IEEE (2019)
13. Cong, R., et al.: Secure interoperation of blockchain and IPFS through client application enabled by CP-ABE. In: Moallem, A. (ed.) HCI for Cybersecurity, Privacy and Trust. HCII 2022. Lecture Notes in Computer Science, vol. 13333, pp. 30–41. Springer, Cham (2022). https://doi.org/10.1007/978-3-031-05563-8_3