Computers, Materials & Continua

Tech Science Press

DOI: 10.32604/cmc.2023.038937
Article

Application of Blockchain Sharding Technology in Chinese Medicine Traceability System

Fuan Xiao[1], Tong Lai[1], Yutong Guan[1], Jiaming Hong[1], Honglai Zhang[1], Guoyu Yang[2] and Zhengfei Wang[1,*]

[1]School of Medical Information Engineering, Guangzhou University of Chinese Medicine, Guangzhou, 510006, China
[2]Institute of Artificial Intelligence and Blockchain, Guangzhou University, Guangzhou, 510006, China
*Corresponding Author: Zhengfei Wang. Email: wzf@gzucm.edu.cn
Received: 04 January 2023; Accepted: 10 April 2023; Published: 09 June 2023

Abstract: Traditional Chinese Medicine (TCM) is one of the most promising programs for disease prevention and treatment. Meanwhile, the quality of TCM has garnered much attention. To ensure the quality of TCM, many works are based on the blockchain scheme to design the traceability scheme of TCM to trace its origin. Although these schemes can ensure the integrity, sharability, credibility, and immutability of TCM more effectively, many problems are exposed with the rapid growth of TCM data in blockchains, such as expensive overhead, performance bottlenecks, and the traditional blockchain architecture is unsuitable for TCM data with dynamic growth. Motivated by the aforementioned problems, we propose a novel and lightweight TCM traceability architecture based on the blockchain using sharding (LBS-TCM). Compared to the existing blockchain-based TCM traceability system, our architecture utilizes sharding to develop a novel traceability mechanism that supports more convenient traceability operations for TCM requirements such as uploading, querying, and downloading. Specifically, our architecture consists of a leader shard blockchain layer as its main component, which employs a sharding mechanism to conveniently TCM tracing. Empirical evaluations demonstrated that our architecture showed better performance in many aspects compared to traditional blockchain architectures, such as TCM transaction processing, TCM transaction querying, TCM uploading, etc. In our architecture, tracing TCM has become a very efficient operation, which ensures the quality of TCM and provides great convenience for subsequent TCM analysis and retrospective research.

Keywords: Blockchain; sharding; traceability; traditional chinese medicine

1 Introduction

Since the outbreak of novel coronavirus pneumonia, traditional Chinese medicine has made great achievements in prevention and treatment. The curative effect of traditional Chinese medicine has attracted more and more public attention [1]. The quality of TCM determines its therapeutic effect,

so the quality and safety of TCM have become a public concern [2]. However, TCM has experienced many intermediate links from planting to consumption, and the information in each circulation link may be tampered with by unscrupulous merchants, which brings severe challenges to the quality and safety of TCM.

Therefore, in the process of TCM from planting to consumption, it is very important to trace the source of circulation information such as planting, production, warehousing, and transportation [3]. People need to record the planting information and origin information in the planting stage, the warehousing and outbound records in the warehousing stage, the manufacturer information and production batch number and other information in the production stage, the information and transaction information of medicinal materials in the circulation stage, and the retail information and patient information when used in the hospital or pharmacy [4]. The whole circulation stage forms a supply chain, which can ensure the quality of TCM and facilitate patients to query whether TCM is counterfeit [5]. In this way, the entire supply chain information forms a traceable system and makes it possible to track the quality, direction, and responsibility of TCM. Traceability can make the public believe that TCM is safe, effective, and quality controllable [6–8]. However, how establishing a trustworthy, efficient, and immutable traceability system to ensure the quality of TCM is still a huge challenge.

Blockchain is a technical solution based on computer technologies such as distributed data storage, point-to-point transmission, consensus mechanism, and encryption algorithm. It is based on a peer-to-peer distributed network and does not need the participation of third-party certification authorities. So all stakeholders involved in the blockchain can share data equally. In addition, it adopts the proof of work (POW) consensus algorithm to ensure the consistency and immutability of data on the blockchain. Data agreed upon based on the consensus algorithm is packaged into blocks, and all blocks are connected into a chain in chronological order [9] to form a blockchain. Each block is composed of a header and a body. The block header contains the field's timestamp, the hash code of the previous block, and the hash code of the root, etc. This chain structure can effectively prevent TCM data tampering and support public audit and traceability.

Due to decentralization and tamper proof, blockchain is widely used in many fields in recent years, such as medicine, food, finance, the Internet of things, etc. [10–12]. Blockchain applications in the medical field mainly focus on medical education, clinical trials, and biomedical research. These fields need to trace the authenticity of the most original data to ensure the safety and availability of medical data [13], which also applies to ensuring the security and availability of TCM data. Specifically, the hashes code of TCM data is produced by the encryption algorithm and saved in the field in the block header, which can prevent the TCM data from being tampered with. The block body mainly contains a series of packaged transactions. In the whole TCM supply chain, all transactions will be packaged and saved in the transaction field by the encryption algorithm. Thus, each TCM transaction data can be traced.

However, building a blockchain-based data traceability system for dynamically changing TCM data still faces a series of performance problems. Because medical data is dynamic and increasing every day [14,15], which makes the amount of data on the blockchain-based medical traceability system also increases, resulting in the continuous exposure of blockchain expansion performance problems, such as huge computing overhead, huge storage overhead, high network latency, and low transaction throughput. These problems are fatal when dealing with emergency medical accidents [16]. Bitcoin [17] and Ethereum [18] are the best proof of the blockchain concept, but the average number of transactions

processed by Bitcoin and Ethereum per second is less than 15, which greatly limits the application of blockchain to other fields.

Sharding is proposed to overcome the performance and scalability limitations of blockchain. The term shard represents a small part of the entire dataset [19]. Sharding scales the blockchain in the horizontal direction, divides the TCM circulation network into multiple sub-shards, and allocates the transaction processing overhead to different sub-shards. Each sub-shard processes part of the transactions without processing the transactions of the whole blockchain, which greatly reduces the circulation cost of stakeholders. Thus, the application of sharding technology to the TCM traceability system based on the blockchain can reduce the storage and computing burden of stakeholders, reduce network latency, improve the throughput of the system, and save TCM data.

In this paper, we propose LBS-TCM, a lightweight blockchain architecture based on sharding. The key contribution of this paper is summarized as follows:

- We apply sharding blockchain to the traceability system of TCM.
- We partition the TCM circulation network into a leader circulation shard network and multiple sub-circulation shard networks. The leader circulation shard network saves the entire state of LBS-TCM. The sub-circulation shard network uploads the entire state of the sub-shards to the leader circulation shard network in the process of circulation.
- We provide a ledger pruning mechanism to reduce the storage overhead of stakeholders in the process of circulation.
- We split cross-shard transactions into intra-shard transactions to reduce the communication overhead of processing cross-shard transactions.

2 Related Work

The traceability system of TCM needs to record the information of the whole circulation link and ensures integrity, sharing, credibility, and immutability. This can ensure the quality and clinical efficacy of TCM [20]. Due to the inherent tamper resistance of blockchain technology, it is widely used in the field of traceability. Blockchain can not only ensure the quality of TCM but also improve the informatization of traditional Chinese medicine [21]. Similarly, blockchain is mainly applied to the medical field to share and safely store data. Table 1 shows the definitions of common key terms used in the paper.

Table 1: Definitions of frequently used key terms

Parameter	Description
LBS-TCM	Lightweight blockchain architecture based on sharding applied to Traditional Chinese medicine
POW	Proof of work
Cross-shard transaction	The inputs of the transaction are from different shards
Intra-shard transaction	The inputs of the transaction are in the same shard
Ledger pruning	Summarizing the entire state of a shard's ledger, reducing the storage and bootstrapping costs for nodes

In the medical traceability system, there are mainly cloud-based traceability and blockchain-based traceability system. Cloud-based traceability systems can provide data interoperability standards for medical data. Arshdeep et al. [22] proposed a cloud-based electronic medical record (EMR) system. The system can provide standard data operation mode for EMR data, as well as data integration and secure access. However, it will face the risk of data tampering.

In medical data traceability systems based on blockchain, blockchain preserves stakeholders' privacy and realizes the sharing and storage of data [23–25]. Wong et al. [26] proposed a clinical trial management system based on blockchain. This system can monitor and ensure the integrity of clinical trial data, resist malicious attacks, make the clinical trial data traceable, immutable, and trustworthy, and help managers audit the trial data. Vazirani et al. [27] proposed an efficient medical record management system based on blockchain. This system maintains the ownership of patient data and protects the privacy of patients. Meanwhile, it also records information on the interaction between patients and doctors through smart contracts. It is important to realize the interoperability of medical records and improve the long-term health results of patients. Dubovitskaya et al. [28] proposed a patient-centric cancer electronic health record data management system based on blockchain. This system can promote the safe and reliable management, sharing, and aggregation of electronic health record (EHR) data, and help patients manage their health data across multiple hospitals. Simultaneously, it can also protect the privacy of patients and allow patients to authorize doctors to view their own electronic health record data. Lee et al. [29] established a management platform for personal health record exchange based on blockchain. This platform is an international personal health data exchange platform, which can ensure the confidentiality, integrity, and availability of health records, and use a variety of data storage modes to solve the problems of security, storage, and transmission of personal health data, to facilitate the cross-international and cross-hospital data exchange between patients and physicians. Liu et al. [30] proposed the privacy protection and data sharing of electronic medical records based on blockchain. This scheme stores the electronic medical record data on the cloud server and the data index on the blockchain, which greatly reduces the risk of data tampering and ensures the security of the data.

In the field of traceability of TCM, Yik et al. [31] proposed the HerBChain blockchain, a platform designed for quality assurance and quality control of traditional Chinese herbal medicines. HerBChain realizes data sharing between pharmaceutical factories and supply chains, and the source and circulation records of traditional Chinese herbal medicines can be traced back. This greatly improves the information transparency between pharmaceutical companies and consumers. Long et al. [32] proposed a blockchain-based traceability system for Chinese medicinal materials. This system combines the seedling, planting, processing, and circulation of Chinese medicinal materials to establish a model for tracing the source of raw materials. Meanwhile, it solves the issues of the traditional traceability system based on the cloud model. The above studies are based on blockchain to realize the integrity, trustworthiness, traceability, and immutability of medical data. Blockchain in these frameworks, however, has poor performance expansion, high computing overhead, low throughput, and high network delay.

Sharding technology can solve the problem of blockchain performance expansion and realize traceability function. Omniledger [33] maintains the long-term security of the blockchain in the different shards and contains a cross-shard submission protocol, which can handle transactions between multiple shards at the atomic level and use transaction processing between different shards and ledger pruning to optimize the performance of the blockchain. RapidChain [34] can resist Byzantine errors of 1/3 participating nodes. To obtain high transaction throughput and ensure the robustness of the blockchain, it uses the cross-shard consensus algorithm and effective cross-shard

transaction authentication technology. In the above schemes, sharding technology is proposed to scale the performance of the blockchain. However, the performance overhead is high when the shard to which the node belongs needs to be reconfigured at the beginning of each epoch. This paper employs TCM leader sharding blockchain, which is responsible for entire state processing on the blockchain and saves the state of the shards to which each stakeholder belongs. Therefore, sharding can improve the performance of the TCM traceability system, such as reducing network latency and improving transaction throughput.

3 Materials and Methods

3.1 Overview of LBS-TCM

In this section, we introduce LBS-TCM which includes a TCM leader sharding and multiple TCM sub-sharding networks. The system architecture is shown in Fig. 1. Leader sharding network includes hospitals, traditional Chinese medicine planting companies, and large pharmaceutical companies, which bear the main burden of the blockchain network and is the core of TCM traceability. In the whole blockchain network, Leader sharding is responsible for maintaining the state of all sub-sharding and providing state queries for the upload and query of TCM data blocks, and reducing the burden on the TCM sub-sharding networks. The TCM sub-sharding network includes patients, TCM pharmacies, and wholesalers of TCM, which provides the traceability interface of TCM for relevant stakeholders and assembles the transaction data structure for the query.

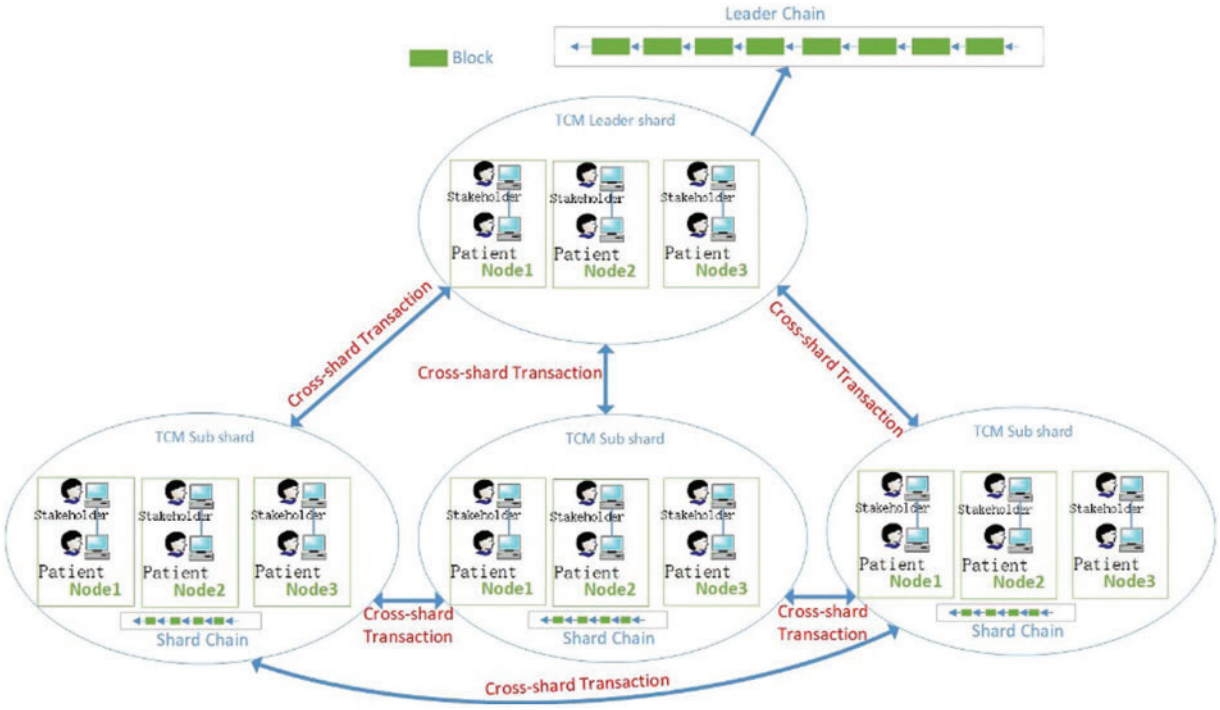

Figure 1: LBS-TCM architecture: TCM leader network with TCM sub-shard networks

3.2 Source of TCM Traceability Data

The Traditional Chinese Medicine data we used was collected from some drugs trade data between farmers, companies, and drug stores, we specifically selected two representative best-selling drugs for testing. The drug data generated from these parties: TCM dealers, patent TCM pharmaceutical production medicine production companies, and raw material sources, have been converted to numeric. The TCM dealers consist of price, approval number, shop name, province, patent TCM pharmaceutical production medicine name, TCM medicine under quality control, and date of sale. The medicines enterprises consist of names of medicines products, main information of raw materials, production enterprises, regions, and TCM medicine under quality control. The source of raw materials: name of production companies, province, the scope of business, herbal TCM medicine under quality control.

3.3 Requirements

LBS-TCM is developed by one or more TCM medical organizations and provides services to patients or pharmacies. LBS-TCM records include planting, production, warehousing, and transportation. TCM manufacturers or hospital upload TCM data to sharding by assembling a transaction. To confirm the authenticity of TCM, TCM retailers or patients can directly connect to the TCM subnetwork in the blockchain network, and send transactions to trace TCM information. LBS-TCM needs to consider the following requirements: (1) Scalability. The storage capability of stakeholders in LBS-TCM should be scalable (2) Integrity. The entire circulation information of TCM should be integral recorded (3) Traceability. TCM circulation information should be tracked in the LBS-TCM architecture. (4) flexibility. The function of the TCM circulation network should be convenient and flexible.

3.4 TCM Leader Sharding Network

The TCM leader blockchain network runs a consensus algorithm to generate TCM leader blocks. The TCM leader block contains information on TCM circulation and sub-sharding state, such as TCM planting information, TCM transaction information, and detection information of TCM, etc. To improve the performance of the system, the TCM leader blockchain network is mainly composed of TCM hospitals, TCM planting companies, and large medical institutions. These structures can withstand the computational overhead, storage overhead, and network connectivity issues in the leader network. The TCM leader blockchain network has three main functions: (1) upload TCM data to the leader blockchain; (2) save the entire state of all sub-TCM shards and provide verification and query for sub-sharding networks; and (3) receive TCM transactions sent by the sub-sharding network. To reduce the burden of the leader-sharding network, we employ pruning technology. The leader-sharding network collects the transactions sent by the sub-sharding network every fixed time, packs them into a block, and inserts the new block into the leader blockchain. Thus, the leader blockchain can process cross-shard transaction queries of TCM and reduce network latency.

3.5 TCM Sub-Sharding Network

The sub-sharding network is composed of patients, dealers, pharmacies, small TCM hospitals, and some inquiry institutions. Each sub-sharding network is responsible for maintaining the state of all participants and processing intra-shard transactions of TCM. The sub-sharding network contains intra-shard TCM transactions and cross-shard TCM transactions. When stakeholders appear in different sub-sharding networks during the circulation and trading of TCM, this is a cross-shard transaction. The ID of each transaction must match the ID of the sub-sharding network where it is

stored. To facilitate patients to trace TCM, patients can connect any node in the sub-sharding network, so that patients do not need to bear high computing overhead and storage overhead. Each sub-shard network will regularly collect intra-shard transactions of TCM, runs a consensus algorithm to create a new sub-shard block, and append the new shard block to its local chain. If a sub-sharding network containing a TCM manufacturer requires to upload TCM data to the traceability system, the sub-shard must send a transaction containing TCM information to the TCM leader sharding network. Sub-sharding blockchains are lightweight blockchains. Thus, the network latency of the system will be very small.

4 Design of LBS-TCM

Compared with the traditional blockchain, the performance of sharding blockchain is better. Therefore, the application of sharding blockchain in the TCM traceability system can improve the speed of processing TCM transactions, reduce the calculation and storage burden of participants in the TCM supply chain, and facilitate patients to trace the quality of TCM. LBS-TCM mainly addresses three main problems: (1) how to shard the participants in the TCM supply chain into corresponding shards; (2) how to process the transactions of TCM circulation; and (3) data operation of TCM traceability.

4.1 The Formation of TCM Supply Chain Network Sharding

In the TCM traceability network based on traditional blockchain, the participants of the TCM supply chain are in the same network, and the participants are not classified. In the TCM supply chain, some Chinese medicine hospitals and Chinese herbal medicine production companies have sufficient hardware facilities to bear the performance consumption in the blockchain network. However, retailers and patients cannot deal with the complex calculation problems in the circulation of TCM. The main function of these participants is to query and access TCM data. Therefore, it is very necessary to shard the participants in the supply chain to optimize the performance of the blockchain. The details of the algorithms of TCM supply chain network sharding are provided in Algorithm 1. The participants are sharded into different shards according to the size and type of the participants. For large TCM manufacturers or TCM hospitals, they can be sharded to the leader-sharding network; However, for TCM retailers or patients, they can be randomly sharded into sub-sharding networks.

Algorithm 1: The formation of TCM supply chain network sharding

Input: the size of shard, attributes of participants in TCM supply chain

```
1. Initializing attribute in participant, set base_size = 32
2. For attribute in participant
3.    If attribute == a patient or a TCM retailer then
4.        Sharding random the participant into sub-shard network
5.    End If
6.    If attribute == a TCM company or hospital then
7.        If size > base_size then
8.            sharding the participant to the leader-sharding network
9.        Else If
10.           sharding random the participant into a sub-sharding network
11.       End If
12.   End If
```

(Continued)

Algorithm 1: Continued

13. **End For**
14. **Output:** TCM sharding network

4.2 TCM Circulation Transaction Processing

The circulation of TCM is completed through the transaction. In the blockchain, the transaction is a field attribute of the block, which is used to save all data operation records. A transaction records the basic information of participants in the supply chain of TCM and the information of TCM, such as the time of the transaction, the name of Chinese herbal medicine, the planting information of Chinese herbal medicine, the name of the manufacturer, the records of patients tracing the source of TCM, etc. For TCM retailers, a transaction records the types of TCM purchased by the retailer, the price of TCM, the purchase time, and the information of the seller. When the shard of the participant in the supply chain and the shard of the target participant is not in the same sharding network, it belongs to a cross-shard transaction, otherwise, it belongs to an intra-shard transaction. The way to handle cross-shard transactions is to split a cross-shard transaction into two intra-shard transactions. This can reduce the communication overhead of the network and improve the performance of the sharding network. The details of the algorithms of TCM circulation transaction processing are provided in Algorithm 2.

Algorithm 2: TCM circulation transaction processing

Input: TCM information, attributes of the participant in the TCM supply chain
1. Identify the type in the participant
2. Construct a transaction in attributes
3. **If** shard_ID == transaction_ID **then**
4. Process the transaction within the shard
5. **Else If**
6. Split the transaction into two intra-transactions
7. **End If**
8. Send the transaction to the target shard
9. **If** the target shard receives the transaction **then**
10. Create a new block and insert the block into the blockchain
11. Alert tips for successful transaction processing
12. **Else If**
13. Alert tips for processing failed
14. **End If**
15. **Output:** Tips for successful transaction processing

4.3 Data Operation of TCM Traceability

The data operation modes of the TCM traceability system mainly include: uploading TCM data, querying, and accessing TCM traceability. In the LBS-TCM, different data operation modes will be provided according to the type of supply chain participants. In the leader sharding network, TCM hospitals can upload TCM data and query the corresponding TCM data. However, in the sub-sharding network, patients or retailers only need to query the data of TCM and do not need to upload the data. This method of distinguishing data operation according to the type of participants can improve the speed of transaction processing of the system. The details of the algorithms for uploading TCM

data are provided in Algorithm 3. To trace TCM information, the participant inputs the unique identification ID, TCM identification ID, and other information related to the traceability of TCM and sends the traceability request to the LBS-TCM system. Then the LBS-TCM receives the request, assembles a new transaction, and sends the transaction to the target shard to be queried. At last, the target shard receives the transaction, queries the TCM information according to the content of the transaction, and returns the queried information to the participant.

Algorithm 3: TCM data uploading

Input: TCM information, attributes of the participant in the TCM supply chain
Output: TCM identification ID, the hash code of the TCM, tips for successful uploading
1. log in to the LBS-TCM system with private_key
2. Input attributes of TCM
3. Send an uploading request to the LBS-TCM
4. LBS-TCM assembles a transaction
5. If shard_ID == transaction_ID **then**
6. Process the transaction and generate the hash code of the TCM
7. Create a new block and insert the block into the blockchain
8. End If
9. Generate a unique ID of TCM
10. **Return** TCM identification ID, the hash code of the TCM, tips for successful uploading

5 Results

We implement LBS-TCM based on Ethereum open source code by using Golang language. The hardware environment is mainly the apple computer, Intel Core i7 processor, 32 GB memory, and 1 T hard disk space. We collected traditional Chinese medicines information produced by different manufacturers. For example the name of TCM products, the main raw materials for the production of TCM, the production enterprise, the scale of the production enterprise, the main business scope of the production enterprise, and the place of production. We uploaded the collected TCM information to the LBS-TCM system for testing. To test the performance of the LBS-TCM system, we compared it with the cloud-based traceability system and the blockchain-based traceability system. We evaluate the performance of the three traceability systems from the following aspects: uploading TCM data, querying TCM data, TCM transaction processing capacity, and storage overhead.

Fig. 2 reports that with the increase of uploading TCM data, the storage overhead of the traceability system also increases. When the data size of TCM data is the same, the storage overhead based on the cloud traceability system is the largest, and the LBS-TCM system is the smallest. In the cloud-based traceability system, all TCM data are stored in the central cloud server, so all storage overhead is reflected in the cloud server, and other participants in the supply chain have no storage overhead. In the blockchain-based traceability system, each participant needs to save TCM data, because each participant needs to run a consistency algorithm to make the TCM data consistent. In the LBS-TCM system, we set up a total of 8 shards, a TCM leader shard, and 7 sub-shards. Each shard saves part of the data of TCM in a decentralized manner, without saving all the data in the whole supply chain. Therefore, the storage overhead is burdened by each shard, and the storage overhead of the whole system will be greatly reduced.

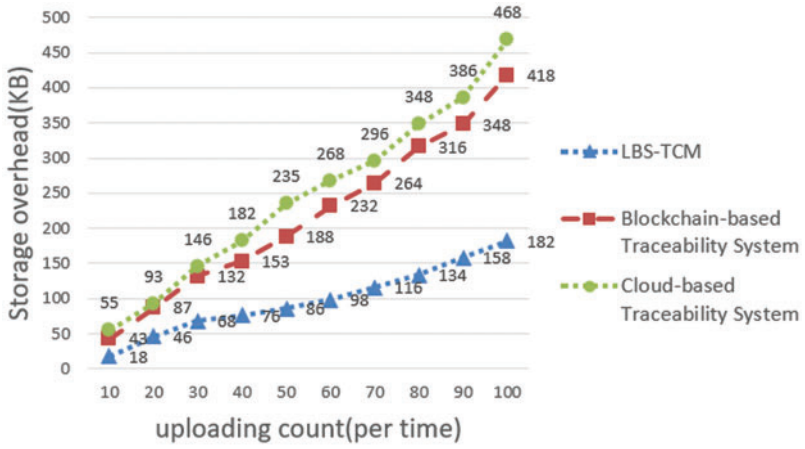

Figure 2: Comparison of storage overhead increases with the uploading of TCM data

Figs. 3 and 4 reveal the response time of uploading TCM data and querying TCM data. With the increase of TCM data, the response time is longer. When the data size of TCM data is the same, the response time of the cloud-based traceability system is longer, and the response time of the LBS-TCM system is the smallest. The response time of the cloud-based traceability system is handled by the central cloud server. Other participants in the TCM supply chain are unable to process it. Therefore, the response time of the cloud-based traceability system will be relatively long. In the blockchain-based traceability system, participants in the TCM supply chain respond to data operations one by one. Because each participant needs to store all the data of TCM. In the LBS-TCM system, the operation of response data is undertaken by the leader-sharding network and sub-sharding networks. Each shard can upload and query TCM data, as well as the saved shard state information, participant account information, and TCM data. Thus, the query and calculation time required is relatively small.

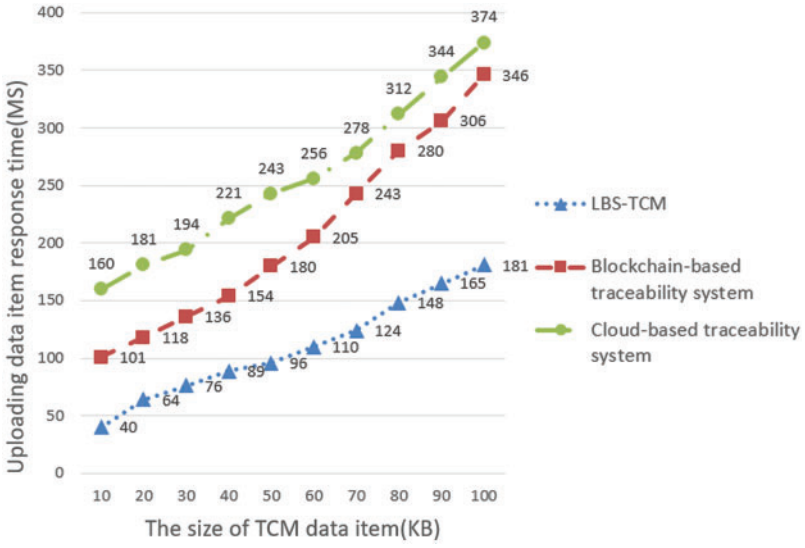

Figure 3: Comparison of time spent uploading TCM data

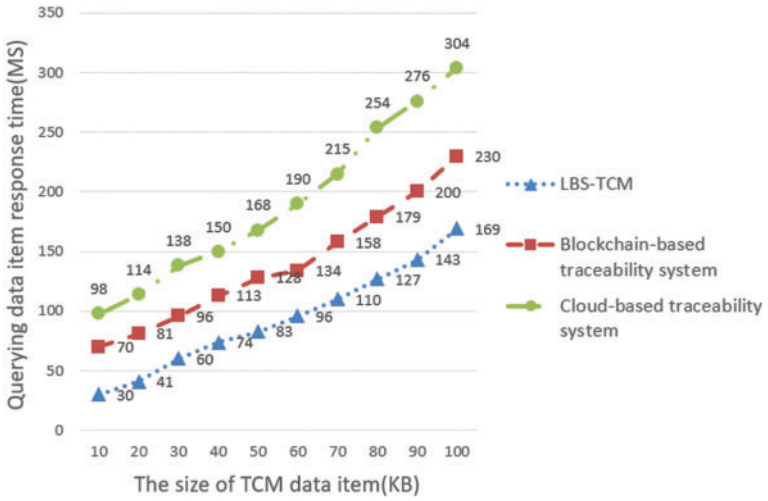

Figure 4: Comparison of time spent querying TCM data

Fig. 5 shows the processing capacity of TCM transactions. The larger the data item of TCM, the weaker the transaction processing ability. Because the TCM data is large, the computing overhead is large, and it takes longer to process the data. In the cloud-based traceability system, other participants cannot provide computing power, all the computing burden is burdened by the central server, so the computing time will be longer. In the blockchain-based traceability system, each generated new block needs to be synchronized to all supply chain participants. Thus, the transaction processing capacity will be relatively weak. In the LBS-TCM system, each shard saves state information and account information and can process transactions, which will take little calculation and query time. In particular, the TCM leader shard saves the state information of all sub-shards, and there is no need to query the information from the sub-shard. Therefore, the transaction processing capacity of TCM will be relatively strong.

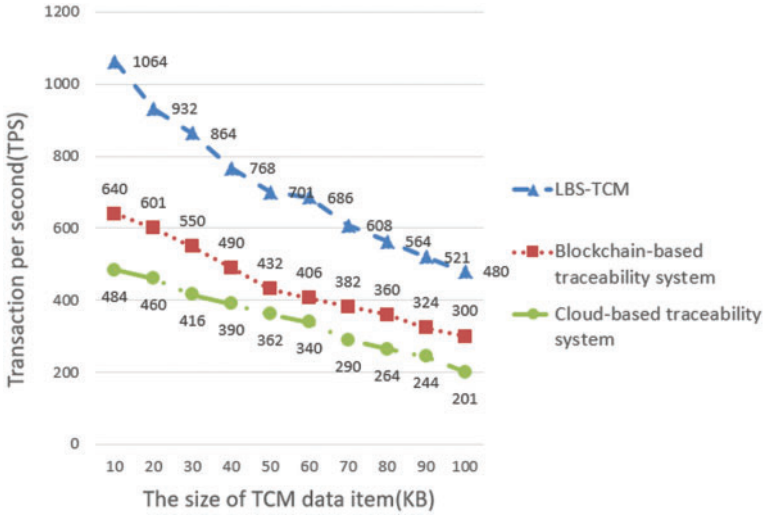

Figure 5: Comparison of TCM transaction processing capacity

6 Discussion

The traceability system of TCM is mainly to ensure the integrity, shareability, credibility, and invariability of TCM. The cloud-based traceability system only saves TCM data on the cloud server [22]. The cloud server is controlled in hospitals or large TCM manufacturers, which leads to the insecurity of TCM data and even face the risk of tampering. TCM data cannot be shared between TCM hospitals. The performance of the system depends entirely on the central cloud server, which leads to low system performance. The traceability system based on blockchain makes use of the characteristics of blockchain to realize the anti-tampering and distributed sharing of TCM data, and the transparent management of TCM data [23]. This makes blockchain widely used in the field of traceability. However, due to the limitations of the blockchain itself, each newly generated block needs to run a consensus algorithm to synchronize with all participants, which leads to low system performance and is not conducive to rapid response data operations. In LBS-TCM System, we employ sharding technology to improve the performance of blockchain and divide the TCM supply chain network into a leader sharding network and a sub-sharding network. In this way, it can be divided into different shards according to the different roles of supply chain participants. Thus, the data operation modes of different participants can be different. The state of each sub-shard is saved in the TCM leader shard. This can reduce the time of each block verification and scale the performance of our framework. Thus, this can reduce the high computation overhead and storage overhead of participants in medical institutions. The experimental data show that sharding technology can improve the performance of the TCM traceability system. Although LBS-TCM implements a lightweight system for blockchain sharding, it still has limitations that we want to address in the future. First, we use a proof of work consensus algorithm on the sub-shard network and the leader-shard network, but it consumes a lot of computing resources and power. We leave to future work the exploration of effective consensus algorithms, such as proof of stake (POS) and practical byzantine fault tolerance (PBFT). Second, LBS-TCM does not formally reason around the motivations of participants but instead focuses on the usual honest or malicious behavior, which leads to an easy attack.

7 Conclusion

We present LBS-TCM, the application of sharding blockchain technology to the TCM that ensures the integrity, sharability, credibility, and immutability of TCM. LBS-TCM is a lightweight client for patients and TCM retailers, the main burden of the system is on hospitals and TCM manufacturers. But LBS-TCM uses TCM leader blockchain, TCM sub-sharding blockchain, and ledger pruning to reduce the burden of hospitals and TCM manufacturers. Finally, our empirical evaluation shows that compared with the blockchain-based traceability system, LBS-TCM can improve the convenience in the operation of TCM traceability data, and greatly improve the performance of TCM data upload, query, and access.

Acknowledgement: Previous medical blockchain applications are the basis of our research. We are thankful to all the researchers and applications that led us to develop a TCM Traceability system.

Funding Statement: This work is supported by the research and innovation program for graduate students of the Guangzhou University of Traditional Chinese Medicine. This work is also partially supported by the National Key Research and Development Program of China (2019YFC1710402), the research on tracing TCM Electronic Medical Records Based on the Lightweight Blockchain of Guangdong Provincial Bureau of Traditional Chinese Medicine (20222045).

Conflicts of Interest: The authors declare that they have no conflicts of interest to report regarding the present study.

References

[1] X. An, Y. Zhang, L. Duan, D. Jin, S. Zhao *et al.,* "The direct evidence and mechanism of traditional Chinese medicine treatment of COVID-19," *Biomedicine & Pharmacotherapy*, vol. 137, pp. 111267, 2021.

[2] C. Zhang, X. Zheng, H. Ni, P. Li and H. -J. Li, "Discovery of quality control markers from traditional Chinese medicines by fingerprint-efficacy modeling: Current status and future perspectives," *Journal of Pharmaceutical and Biomedical Analysis*, vol. 159, pp. 296–304, 2018.

[3] L. -L. Dong, Y. -G. Duan, B. Wang, C. -Q. Wang, G. -F. Wei *et al.,* "Management system and development strategy of quality Chinese medicine," *China Journal of Chinese Materia Medica*, vol. 46, no. 17, pp. 4307–4313, 2021.

[4] M. He and J. Shi, "Circulation traceability system of Chinese herbal medicine supply chain based on internet of things agricultural sensor," *Sustainable Computing: Informatics and Systems*, vol. 30, pp. 100518, 2021.

[5] S. M. Yi, L. C. Yu, W. C. Biao, X. Xiong and L. S. Nan, "Design and development of quality traceability system for circulation of Chinese herbal medicine based on blockchain and NB-IOT," *China Journal of Chinese Materia Medica*, vol. 45, no. 17, pp. 4267–4272, 2020.

[6] S. Zhou, H. Sheng, J. Ma and X. Han, "Review of the application of blockchain technology in traditional Chinese medicine field," in *Proc. of the 2020 Int. Symp. on Artificial Intelligence in Medical Sciences*, Beijing, China, pp. 225–230, Association for Computing Machinery, 2020.

[7] L. Zhao, J. Zhang and H. Jing, "Blockchain-enabled digital rights management for museum-digital property rights," *Intelligent Automation & Soft Computing*, vol. 34, no. 3, pp. 1785–1801, 2022.

[8] J. Zhu, C. Yan, Y. Ouyang, Y. Chen and X. Wang, "Security data sharing of shipbuilding information based on blockchain," *Intelligent Automation & Soft Computing*, vol. 33, no. 3, pp. 1747–1756, 2022.

[9] Z. Wang, L. Wang, F. A. Xiao, Q. Chen, L. Lu *et al.,* "A traditional Chinese medicine traceability system based on lightweight blockchain," *Journal of Medical Internet Research*, vol. 23, no. 6, pp. e25946, 2021.

[10] M. Xu, X. Chen and G. Kou, "A systematic review of blockchain," *Financial Innovation*, vol. 5, no. 1, pp. 27, 2019.

[11] J. -M. Alanazi and A. -A. AlZubi, "An optimized method for information system transactions based on blockchain," *Intelligent Automation & Soft Computing*, vol. 35, no. 2, pp. 2289–2308, 2023.

[12] D. D. H. Miriam, D. Dahiya, Nitin and C. R. R. Robin, "Secured cyber security algorithm for healthcare system using blockchain technology," *Intelligent Automation & Soft Computing*, vol. 35, no. 2, pp. 1889–1906, 2023.

[13] Y. Xie, J. Zhang, H. Wang, P. Liu, S. Liu *et al.,* "Applications of blockchain in the medical field: Narrative review," *Journal of Medical Internet Research*, vol. 23, no. 10, pp. e28613, 2021.

[14] A. A. Vazirani, O. O—Donoghue, D. Brindley and E. Meinert, "Implementing blockchains for efficient health care: Systematic review," *Journal of Medical Internet Research*, vol. 21, no. 2, pp. e12439, 2019.

[15] J. Priya and C. Palanisamy, "Novel block chain technique for data privacy and access anonymity in smart healthcare," *Intelligent Automation & Soft Computing*, vol. 35, no. 1, pp. 243–259, 2023.

[16] H. X. Son, T. H. Le, N. T. T. Quynh, H. N. D. Huy, N. Duong-Trung *et al.,* "Toward a blockchain-based technology in dealing with emergencies in patient-centered healthcare systems," in *2020 Int. Conf. on Mobile, Secure, and Programmable Networking*, Cham, Switzerland, pp. 44–56, 2020.

[17] S. Nakamoto and A. Bitcoin, "A peer-to-peer electronic cash system," vol. 4, 2008. *Bitcoin.–URL*: https://bitcoin.org/bitcoin.pdf

[18] G. Wood, "Ethereum: A secure decentralised generalised transaction ledger," *Ethereum Project Yellow Paper*, vol. 151, no. 2014, pp. 1–32, 2014.

[19] G. Wang, Z. J. Shi, M. Nixon and S. Han, "SoK: Sharding on blockchain," in *Proc. of the 1st ACM Conf. on Advances in Financial Technologies*, Zurich, Switzerland, pp. 41–61, 2019.

[20] W. Yang, Y. Zhang, W. Wu, L. Huang, D. Guo *et al.,* "Approaches to establish Q-markers for the quality standards of traditional Chinese medicines," *Acta Pharmaceutica Sinica B*, vol. 7, no. 4, pp. 439–446, 2017.
[21] L. Peng, "Application of blockchain in the field of traditional Chinese medicine," in *2019 Int. Conf. on Information Technology and Computer Application*, Guangzhou, China, pp. 319–322, 2019.
[22] B. Arshdeep and K. M. Vijay, "A cloud-based approach for interoperable electronic health records (EHRs)," *IEEE Journal of Biomedical and Health Informatics*, vol. 17, no. 5, pp. 894–906, 2013.
[23] H. Yan, N. Jiang, K. Li, Y. Wang and G. Yang, "Collusion-free for cloud verification toward the view of game theory," *ACM Transactions on Internet Technology (TOIT)*, vol. 22, no. 2, pp. 1–21, 2021.
[24] G. Lin, H. Yan, G. Kou, T. Huang, S. Peng *et al.,* "Understanding adaptive gradient clipping in DP-SGD, empirically," *International Journal of Intelligent Systems*, vol. 37, no. 11, pp. 9674–9700, 2022.
[25] R. Hou, S. Ai, Q. Chen, H. Yan, T. Huang *et al.,* "Similarity-based integrity protection for deep learning systems," *Information Sciences*, vol. 601, pp. 255–267, 2022.
[26] D. R. Wong, S. Bhattacharya and A. J. Butte, "Prototype of running clinical trials in an untrustworthy environment using blockchain," *Nature Communications*, vol. 10, no. 1, pp. 917, 2019.
[27] A. A. Vazirani, O. O'Donoghue, D. Brindley and E. Meinert, "Blockchain vehicles for efficient medical record management," *NPJ Digital Medicine*, vol. 3, no. 1, pp. 1–5, 2020.
[28] A. Dubovitskaya, F. Baig, Z. Xu, R. Shukla, P. S. Zambani *et al.,* "Action-EHR: Patient-centric blockchain-based electronic health record data management for cancer care," *Journal of Medical Internet Research*, vol. 22, no. 8, pp. e13598, 2020.
[29] H. -A. Lee, H. -H. Kung, J. G. Udayasankaran, B. Kijsanayotin, A. B. Marcelo *et al.,* "An architecture and management platform for blockchain-based personal health record exchange: Development and usability study," *Journal of Medical Internet Research*, vol. 22, no. 6, pp. e16748, 2020.
[30] J. Liu, X. Li, L. Ye, H. Zhang, X. Du *et al.,* "BPDS: A blockchain based privacy-preserving data sharing for electronic medical records," in *2018 IEEE Global Communications Conf.*, Abu Dhabi, United Arab Emirates, pp. 1–6, 2018.
[31] M. H. -Y. Yik, V. C. -W. T. Wong, T. -H. Wong and P. C. Shaw, "HerBChain, a blockchain-based informative platform for quality assurance and quality control of herbal products," *Journal of Traditional and Complementary Medicine*, vol. 11, no. 6, pp. 598–600, 2021.
[32] Y. Long, D. Chu, H. Wang, J. Fu and H. Yan, "Blockchain-based trace the source system for Chinese medicinal materials," in *14th Int. Conf. on Measuring Technology and Mechatronics Automation*, Changsha, China, pp. 1007–1010, 2022.
[33] E. Kokoris-Kogias, P. Jovanovic, L. Gasser, N. Gailly, E. Syta *et al.,* "OmniLedger: A secure, scale-out, decentralized ledger via sharding," in *2018 IEEE Symp. on Security and Privacy*, San Francisco, CA, USA, pp. 583–598, 2018.
[34] M. Zamani, M. Movahedi and M. Raykova, "RapidChain: Scaling blockchain via full sharding," in *Proc. of the 2018 ACM SIGSAC Conf. on Computer and Communications Security*, Toronto, Canada, pp. 931–948, 2018.