International Journal of Applied Science; Vol. 8, No. 1; 2025
ISSN 2576-7240 E-ISSN 2576-7259
https://doi.org/10.30560/ijas.v8n1p98

Blockchain-based Traditional Chinese Medicine Traceability Model

Bo Li[1], Xiaowei Yuan[1], Wangyu Liao[1], Yang Yuan[1] & Xue Yan[1]

[1] School of Information and Engineering, Sichuan Tourism University, China

Correspondence: Xue Yan, School of Information and Engineering, Sichuan Tourism University, Chengdu, 610100, China. E-mail: 13368545@qq.com

Received: March 19, 2025; Accepted: March 30, 2025; Published: March 31, 2025

Abstract

Traditional Chinese medicine is widely used in the medical field for its good curative effect and extremely small side effects,but the sources and preparation processes of traditional Chinese medicine materials lack transparency,Some traditional Chinese medicines have the defects of being easy to counterfeit and difficult to trace.Thus, a blockchain-based traditional Chinese medicine traceability model(BTCMT) is proposed in the paper.This model is based on the blockchain and uses a distributed storage mechanism. Under the control of the practical Byzantine algorithm and smart contract, it has achieved the distributed management of the whole process of planting, collecting, primary processing, preparation and sales of traditional Chinese medicine, ensuring the transparency, decentralization and anti-counterfeiting of traditional medicine on each block, and has realized the traceability and information sharing of traditional Chinese medicine. After simulation experiments, the accounting success rate of BTCMT was 100%, Failure rate is 0%, the shortest traceability response time was 212ms, and the maximum system traceability throughput was 4908.02bps. The model has good robustness and provides a reference for the traceability model of traditional Chinese medicine.

Keywords: blockchain, Traditional Chinese medicine traceability, traceability model

1. Introduction

Traditional Chinese medicine（TCM） has a history of more than 5,000 years and is a unique creation of China. It is widely used all over the world occupies an important position in the world's medical system. But it is prone to problems in planting, collection, preparation, storage and other links, which directly affects the efficacy and quality of traditional Chinese medicine. Therefore, traceability of traditional Chinese medicine becomes necessary, it can accurately find problems, and compared with ordinary centralized management, BTCMT has the advantages of distribution, decentralization and non-tampering, and has attracted much attention.

Q Xu[1] clearly pointed out that the blockchain is a good way to achieve the anti-counterfeiting and traceability of traditional Chinese medicine, demonstrated the applicability of the blockchain to the traceability of traditional Chinese medicine, and determined the feasibility of the blockchain in the traceability of traditional Chinese medicine. Yin F F[2] proposed the use of blockchain technology in the anti-counterfeiting of drugs, which has excellent performance and gives theoretical basis, is superior to the centralized management system, and the use of blockchain in the traceability of traditional Chinese medicine has been recognized and demonstrated from a theoretical point of view. S Zhou[3] also explicitly pointed out that the inevitable trend of TCM access and traceability is blockchain, affirming the prospects of blockchain in the T traceability system from the aspects of practical feasibility and technical feasibility.

Moreover, Scott N A [4] proposed a drug optimization inventory management system, but this method is limited to the optimization of traditional Chinese medicine inventory, and a management approach is adopted, which can achieve the traceability of traditional Chinese medicine, but this method is over-centralized and has the defects of tampering and unsupervised defects. DattaSagnik and NamasudraSuyel [5] proposed a management method for the transportation of traditional Chinese medicine, which adopted the blockchain, but it was limited to the safe transportation of traditional Chinese medicine, and did not cover the entire process of traditional Chinese medicine, which was of great limitations. Wang Z [6] proposed a lightweight blockchain-based traditional Chinese medicine traceability framework, which can combat the phenomenon of fake drugs and achieve drug traceability, the theory and methods in this framework are only implemented in lightweight traditional Chinese medicine traceability, and there are obvious restrictions on functions and performance.

In view of the above limitations and shortcomings, this paper proposes a universal, functional and high-performance traditional Chinese medicine blockchain model, namely BTCMT, which can achieve the anti-counterfeiting and traceability of traditional Chinese medicine.

2. Model and method

2.1 The Structure of Block

In the BTCMT model, the block is the main component and the carrier of accounting information, which records detailed information about traditional Chinese medicine. The blocks are deployed each node, and the distributed completion of information accounting and on-chain is achieved. The traceability of traditional Chinese medicine is realized by inquiring the information in the block. core of the block is supported by a Merkle tree based on hash256, as shown in Figure 1.

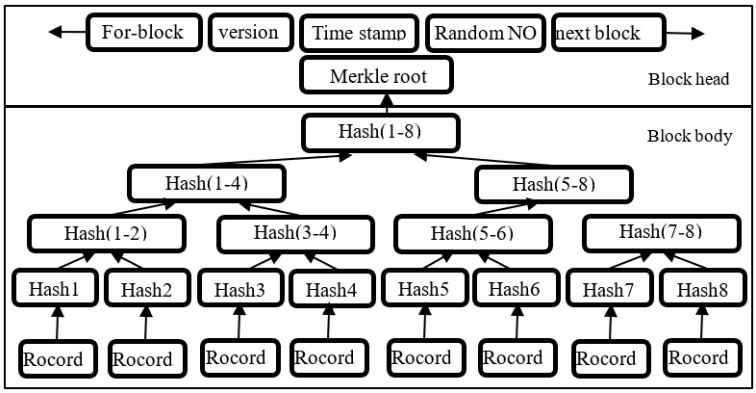

Figure 1. Block structure diagram based on Merkle tree

As can be seen from Fig. 1, the traditional Chinese medicine block is divided into two parts, i.e., the block head and the block body, and for-block and next-block in the head enable all the blocks to be connected to form a blockchain. The core of the block is the Merkle support tree, where the record represents the accounting information of traditional Chinese medicine, is the leaf node of the Merle tree, the leaf node must be even, if it is odd, the last node is copied once, making up an even number of nodes, and the hash value of the upper node is calculated by the hash256 algorithm of the two lower nodes, Likewise, iterating upwards one by one, the hash value of the root node can be calculated in the end. So, Any modification of the accounting information of a leaf node will result in a change in the hash value of the root node. By traversing the nodes, the nodes can be quickly discovered and located. The modified information must be authorized by the smart contract to be recognized by the blockchain and maintain consistency with all other nodes. This is obviously impossible so it can effectively prevent the accounting information of traditional Chinese medicine from being tampered with and ensure the consistency and immutability of the information in the block.

2.2 Distributed Storage Model for Blockchain, DSB

The distributed storage is highly consistent with the distributed characteristics of the blockchain, which avoids excessive centralization, achieves decentralization, and improves the security of the traditional Chinese medicine blockchain. The structure of DSB is shown in Figure 2.

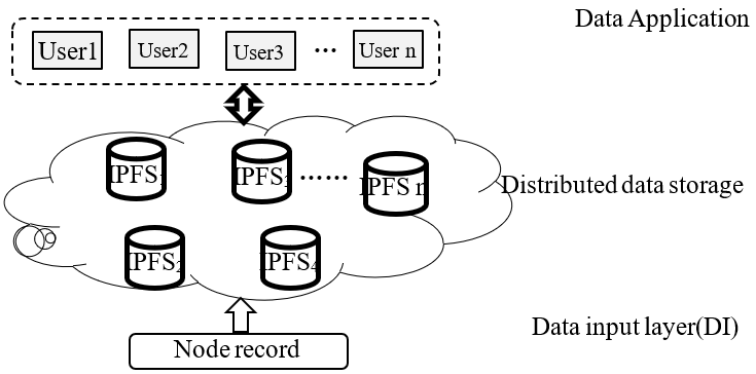

Figure 2. Structure of DSB

From Figure 2, we can see that DSB is divided into three layers, which are Data input layer (DI), Distributed data storage layer (DS), and Data Application Layer (DA).

1. Data input layer, DI

DI is responsible for the entry of TCM accounting information, which is the main way of data collection in the TCM blockchain. TCM information is entered through to form accounting information, and the accounting information is completed on the chain under the recognition of smart contracts, providing data query services for subsequent traceability.

2. Distributed data storage layer, DS

DDS uses IPFS technology, when searching for data, IPFS can verify the hash value of the target data to complete the access to the target data. addition, in IPFS, once the data changes, such as illegal operations like tampering, its hash value will also change accordingly, thus, IPFS ensures the immutability security and irreversibility of the data, and provides a security guarantee for data storage in the blockchain, which is highly suitable for the distributed storage structure of the blockchain.

3. Data Application Layer, DA

DA provides users with information inquiry and traceability. DA is responsible for accepting the user's access request, forwarding the request to the lower layer, and also the data information to the user. It is the interface for interaction between the user and DSB.

2.3 Blockchain-Based Traditional Chinese Medicine Traceability Model, BTCMT

Blocks and distributed storage systems are important components of the BTCMT model, which implement the main functions of the blockchain and provide pharmaceutical traceability services for users, realizing query, traversal, and verification of ledger information, etc. The system structure of BTCMT is shown in Figure 3.

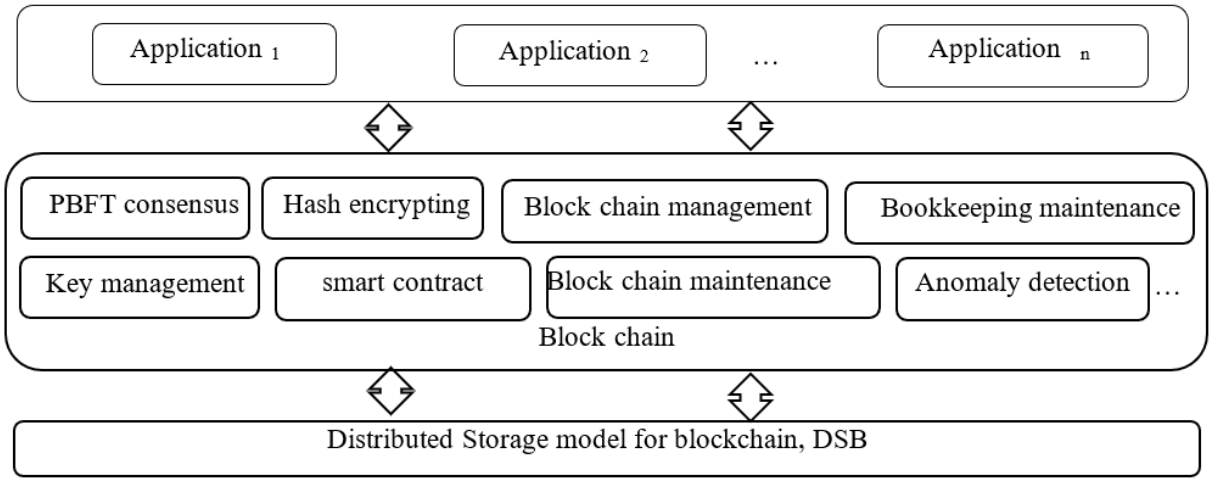

Figure 3. Structure of BTCMT

As can be seen from Fig. 3, the BTCMT model includes three layers, the first is DSB, which implements distributed storage of data. The second layer is the blockchain layer, which is responsible for implementing the BPFT consensus, account book on-chain, smart contract, ledger maintenance, block management etc., and is the core of the BTCMT system. The third layer is the application layer, which provides users with an interface for traceability. These layers cooperate with each other, and under the action of smart contracts and Byzantine algorithm, the traceability of traditional Chinese medicine is completed, and it is shown in Figure 4.

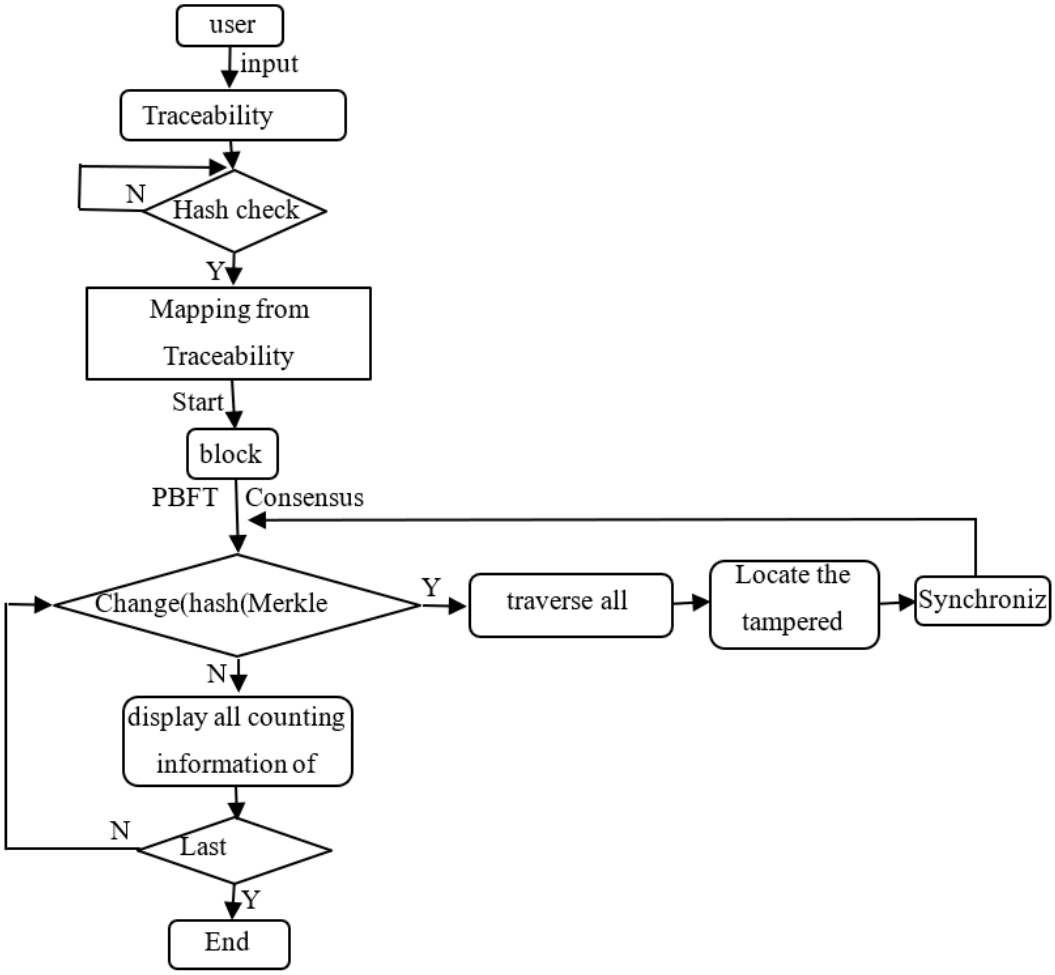

Figure 4. Diagram of BTCMT

As shown in Fig. 4, the process of traceability is divided into the following 3 steps.

Step 1, the user inputs the traceability code, the system performs a hash check on the traceability code, and after the check is passed, the system the head address of the blockchain from the mapping table, and then accesses the first block.

Step 2, when visiting a block, first check whether the hash value of the Merkle root node has changed. If it has changed, which indicates the information in this block has been tampered with, then traverse all nodes in the tree, locate the node where the information is modified and report it. Otherwise, query detailed information of this block.

Step 3, after visiting a block, access the next block according to the back pointer in the block header, and loop to perform the step 2. When all blocks have been traversed, the traceability of traditional Chinese medicine is completed.

The algorithm of BTCMT is shown as follows.

```
1  If   Hash(trac_code)==true then go3;            // check hash code.
2  Else print("trac_code is error!");
3  adr= address(head) from mapping_table;      //get the head address of block chain.
4  While
5  {
6  run PBFT consensus;
7  If change(hash(Merkle_root)= =true,then 7;    //Check if the hash value of the root node of the Merkle
tree has been changed.
8  For(b1=root; node++;b1=end)
```

```
9  {
10 If change(hash(node))==true,then go to 10
11 Print("the node is Untrustworthy",node_no);
12 Else node++;
13 }
14 Else
15 Print("all accounting information is followed:", inf); //display all information.
16 next block;
17 Go 7;        // access the next block
18 };
19 End while;
```

In this algorithm, each time a block is visited, it is necessary to check whether the value of the Merkle tree root node has changed. If it changed, locate and report an error. If it has not changed, get the block information. The loop can complete the access to all blocks.

3. Empirical Analysis

In order to carry out simulation experiments, An experimental platform was built，the Hardware configuration is: Lenovo Tianyi 610 series computer, Intel i5-11400, main frequency 5.0GH, hard disk capacity 2TB, memory 320GB, dedicated graphics card 3GB; Software configuration is as follows: Windows 10 system platform, the front-end web of the traceability system uses SSH framework, Tomcat server, JAVA and MyEclipse compilation system.

Since this experiment is a simulation experiment, using the core test data, Fabric V1.0, which is concise and mature, is used. In addition, and Git, etc., are used as system components of the blockchain environment, and Go language and GoLand compilation system are used as the support of the blockchain, and the practicalantine fault-tolerant algorithm PBFT is used as the consensus algorithm.

In order to demonstrate the rationality, effectiveness and availability of the food traceability system，according to the above experimental environment and platform deployment，the experiments of uploading ledger to the chain，traceability query and abnormal alarm were carried out respectively，and the performance test and data analysis were carried out from the aspects of delay，accuracy， time and system throughput，so as to demonstrate the performance of the traceability system from multiple perspectives.

3.1 Accounting Efficiency Analysis

Accounting efficiency is the efficiency of ledger information on the chain, which refers to the efficiency of accounting information being recognized by the consensus mechanism of the traditional Chinese blockchain and being officially recorded in the block throughout the entire blockchain, and is a performance indicator of the traditional Chinese medicine traceability system. Here, KylinPET is used to multiple terminals issuing ledger information on-chain requests, and its efficiency is shown in Table 1.

Table 1. Summary of Accounting Efficiency

REQUEST	RESPONCE	IDENTIFICATION	MIN(ms)	MAX(ms)	AVG(ms)	THROUGHPUT
500	500	5	161	24095	12128	270.52
1000	1000	5	168	25141	12655	559.82
1500	1500	5	180	30298	15239	903.75
2000	2000	5	179	31617	15898	1004.74
2500	2500	5	201	38020	19211	1206.80
3000	3000	5	231	40940	30586	980.43
3500	3500	5	238	41084	31210	1032.85
4000	4000	5	242	45097	32781	1506.32

It can be seen from Table 1 that the system response success rate is 100%, and there is no response failure. With the increase of requests, the minimum and maximum delays are both within a reasonable range, and the average delay increases slowly with the increase of requests, which can better complete the accounting task, the average delay chart is shown in Figure 5.

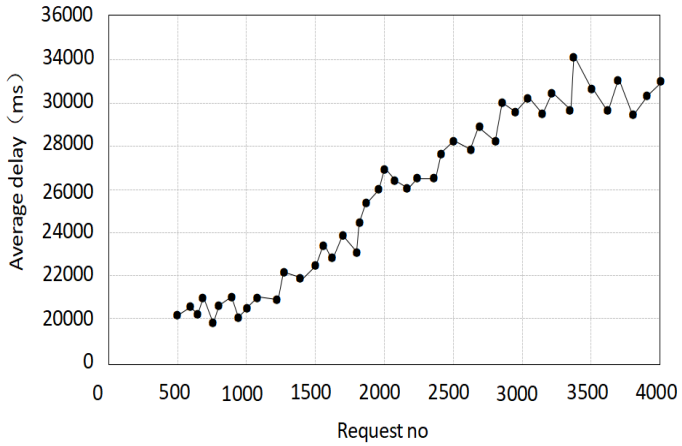

Figure 5. Average delay chart of BTCMT

It can be seen from the data in Table 1 that as the number of accounting requests increases, the throughput of the system increases slightly and shows a stable trend, reflects the stability of the BTCM model, as shown in Figure 6.

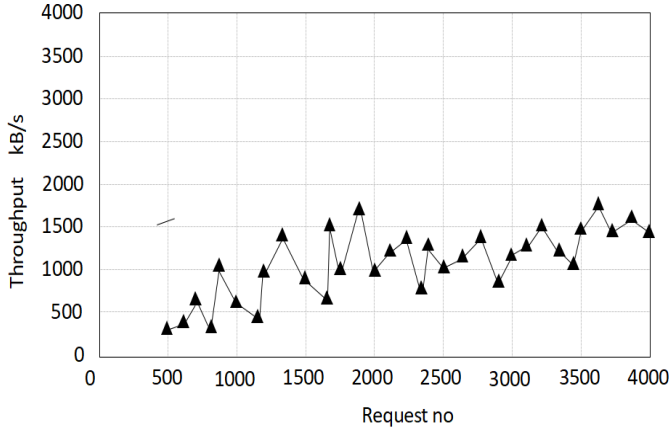

Figure 6. throughput chart of BTCMT

As can be seen from Fig. 5 and Fig. 6, when the number of terminal requests increases, the average response time of the upper chain also increases, and the system is also increasing, the curve changes normally, and all of them are within the system can handle the range, it can be seen that the system has good feasibility and stability.

3.2 Traceability Efficiency Analysis

Traceability is the core function of BTCMT, and it is also a core indicator to measure the performance of the model. When the number of requests increases, its latency and the corresponding value of system throughput are shown in Table 2.

Table 2. Traceability Efficiency Summary

REQUEST	RESPONCE	ERROR	MIN(trace time)	MAX(trace time)	AVG(trace time)	THROUGHPUT
500	500	0	212	9018	8012	2061.07
1000	1000	0	251	10029	8357	3129.54
1500	1500	0	243	12870	9502	3508.42
2000	2000	0	268	13429	10329	3821.83
2500	2500	0	240	15298	12840	4047.06
3000	3000	0	279	17661	15509	4419.72
3500	3500	0	301	18783	17706	4708.51
4000	4000	0	341	20116	18420	4908.02

The data in Table 2 show that the number of BTCMT's trace failure is 0, and the average trace time and system throughput with the increase the number of requests are shown in the curve as shown in Fig. 7 and Fig.8, the security of the trace model is high, and the change of the curve is normal, the performance of the model is stable.

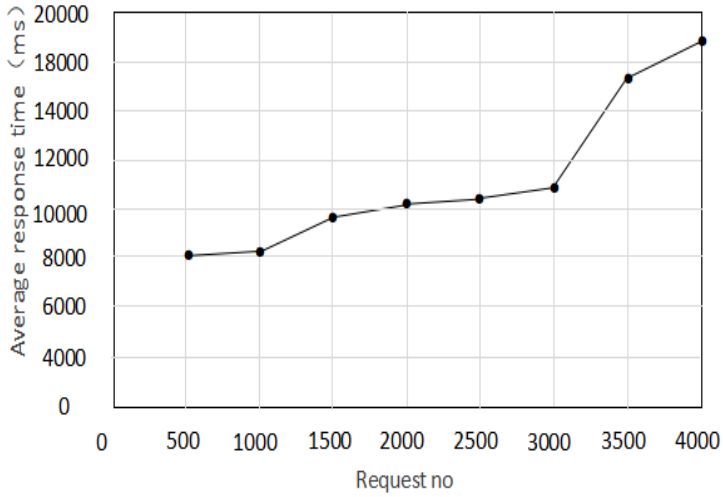

Figure 7. Average Response Time Diagram

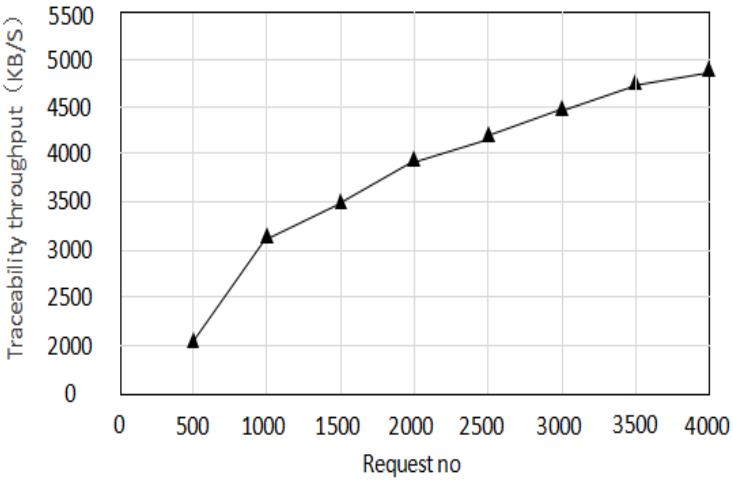

Figure 8. Traceability Throughput Diagram

From Figure 7 and Figure 8, it can be seen that when the number of requests increases, both the average latency and throughput of BTCMT increase, amplitude of the curve is gentle, and there is no sudden sharp increase or decrease, all changes are in line with the normal situation of BTCMT, which reflects that BTCMT has stability, security and feasibility during the work.

4. Conclusion

Traditional traceability system has shortcomings such as centralization, centralization, tampering and insecurity, while the blockchain-based traditional Chinese medicine traceability system avoids these defects and has the advantages of decentralization, distribution, non-tampering and convenient traceability. From the results of simulation experiments, BTCMT has obvious advantages.

1. The BTCMT model is feasible in terms of technology and design, with a complete development environment and a feasible technical scheme.

2. BTCMT has an effect rate of 100% and an error rate of 0%, showing the correct system functionality, stable operation, and good robustness.

3. BTCMT also exhibits good performance in terms of delay, response time, and system throughput, and its various performances are all within a reasonable range.

Acknowledgement

This paper is supported by the university-level project [2021]SCTUZK82 and the university-level Scientific Research Innovation Team Project [2021]SCTUTP03 of Sichuan Tourism University.

References

[1] Xu, Q., Bauer, R., Hendry, B. M., et al. (2013). The quest for modernisation of traditional Chinese medicine. *BMC Complementary and Alternative Medicine, 13*, 132. https://doi.org/10.1186/1472-6882-13-132

[2] Yin, F. F., & Ching, L. Y. (2015). Developing traditional Chinese medicine in the era of evidence-based medicine: Current evidences and challenges. *Evidence-Based Complementary and Alternative Medicine, 2015*(425037), 1-9. https://doi.org/10.1155/2015/425037

[3] Zhou, S., Sheng, H., Ma, J., et al. (2020). Review of the application of blockchain technology in traditional Chinese medicine field. *Proceedings of the 2020 International Conference on Blockchain Technology*. https://doi.org/10.1145/3429889.3429932

[4] Scott, N. A., Lee, K. K., Sadowski, C., et al. (2021). Optimizing drug inventory management with a web-based information system: The TBTC Study 31/ACTG A5349 experience. *Contemporary Clinical Trials, 105*, 106377. https://doi.org/10.1016/j.cct.2021.106377

[5] Datta, S., & Namasudra, S. (2024). Blockchain-based secure and scalable supply chain management system to prevent drug counterfeiting. *Cluster Computing*. https://doi.org/10.1007/s10586-024-04417-3

[6] Wang, Z., Wang, L., Xiao, F., et al. (2021). A traditional Chinese medicine traceability system based on lightweight blockchain. *Journal of Medical Internet Research, 23*(6), e25946. https://doi.org/10.2196/25946